

PATENT ASSIGNMENT COVER SHEET

Electronic Version v1.1
 Stylesheet Version v1.2

EPAS ID: PAT6611692

SUBMISSION TYPE:	NEW ASSIGNMENT	
NATURE OF CONVEYANCE:	SECURITY INTEREST	
CONVEYING PARTY DATA		
Name		Execution Date
HART INTERCIVIC, INC.		03/18/2021
RECEIVING PARTY DATA		
Name:	SILICON VALLEY BANK	
Street Address:	3003 TASMAN DRIVE	
City:	SANTA CLARA	
State/Country:	CALIFORNIA	
Postal Code:	95054	
PROPERTY NUMBERS Total: 18		
Property Type	Number	
Patent Number:	6827262	
Patent Number:	6873966	
Patent Number:	7032821	
Patent Number:	7216807	
Patent Number:	8985435	
Patent Number:	10505801	
Patent Number:	10438433	
Patent Number:	D823336	
Patent Number:	10169943	
Patent Number:	10445966	
Patent Number:	10573111	
Application Number:	13967054	
Application Number:	14817317	
Application Number:	15242784	
Application Number:	29653559	
Application Number:	16517011	
Application Number:	16745621	
Application Number:	62932554	
CORRESPONDENCE DATA		

Fax Number:

Correspondence will be sent to the e-mail address first; if that is unsuccessful, it will be sent using a fax number, if provided; if that is unsuccessful, it will be sent via US Mail.

Phone: (619) 699-2708
Email: christian.cruz@us.dlapiper.com
Correspondent Name: DLA PIPER LLP (US)
Address Line 1: 401 B STREET
Address Line 2: SUITE 1700
Address Line 4: SAN DIEGO, CALIFORNIA 92101

NAME OF SUBMITTER:	MATT SCHWARTZ
SIGNATURE:	/s/ Matt Schwartz
DATE SIGNED:	03/19/2021
	This document serves as an Oath/Declaration (37 CFR 1.63).

Total Attachments: 7

source=SVB_-_Hart_InterCivic,_Inc._-_Intellectual_Property_Security_Agreement_(3.2021).DOCX#page1.tif
source=SVB_-_Hart_InterCivic,_Inc._-_Intellectual_Property_Security_Agreement_(3.2021).DOCX#page2.tif
source=SVB_-_Hart_InterCivic,_Inc._-_Intellectual_Property_Security_Agreement_(3.2021).DOCX#page3.tif
source=SVB_-_Hart_InterCivic,_Inc._-_Intellectual_Property_Security_Agreement_(3.2021).DOCX#page4.tif
source=SVB_-_Hart_InterCivic,_Inc._-_Intellectual_Property_Security_Agreement_(3.2021).DOCX#page5.tif
source=SVB_-_Hart_InterCivic,_Inc._-_Intellectual_Property_Security_Agreement_(3.2021).DOCX#page6.tif
source=SVB_-_Hart_InterCivic,_Inc._-_Intellectual_Property_Security_Agreement_(3.2021).DOCX#page7.tif

INTELLECTUAL PROPERTY SECURITY AGREEMENT

This Intellectual Property Security Agreement ("Agreement") is entered into as of March 18, 2021, by and between SILICON VALLEY BANK, a California corporation ("Bank"), and HART INTERCIVIC, INC., a Texas corporation ("Grantor").

RECITALS

A. Bank has agreed to make certain advances of money and to extend certain financial accommodation to Grantor (the "Loans") in the amounts and manner set forth in that certain Loan and Security Agreement by and between Bank and Grantor dated the Effective Date (as the same may be amended, modified or supplemented from time to time, the "Loan Agreement"; capitalized terms used herein are used as defined in the Loan Agreement). Bank is willing to make the Loans to Grantor, but only upon the condition, among others, that Grantor shall grant to Bank a security interest in certain Copyrights, Trademarks, Patents, and Mask Works (as each term is described below) to secure the obligations of Grantor under the Loan Agreement.

B. Pursuant to the terms of the Loan Agreement, Grantor has granted to Bank a security interest in all of Grantor's right, title and interest, whether presently existing or hereafter acquired, in, to and under all of the Collateral.

NOW, THEREFORE, for good and valuable consideration, receipt of which is hereby acknowledged, and intending to be legally bound, as collateral security for the prompt and complete payment when due of its obligations under the Loan Agreement, Grantor hereby represents, warrants, covenants and agrees as follows:

AGREEMENT

1. Grant of Security Interest. To secure its obligations under the Loan Agreement, Grantor grants and pledges to Bank a security interest in all of Grantor's right, title and interest in, to and under its intellectual property (all of which shall collectively be called the "Intellectual Property Collateral"), including, without limitation, the following:

(a) Any and all copyright rights, copyright applications, copyright registrations and like protections in each work or authorship and derivative work thereof, whether published or unpublished and whether or not the same also constitutes a trade secret, now or hereafter existing, created, acquired or held, including without limitation those set forth on Exhibit A attached hereto (collectively, the "Copyrights");

(b) Any and all trade secrets, and any and all intellectual property rights in computer software and computer software products now or hereafter existing, created, acquired or held;

(c) Any and all design rights that may be available to Grantor now or hereafter existing, created, acquired or held;

(d) All patents, patent applications and like protections including, without limitation, improvements, divisions, continuations, renewals, reissues, extensions and continuations-in-part of the same, including without limitation the patents and patent applications set forth on Exhibit B attached hereto (collectively, the "Patents");

(e) Any trademark and servicemark rights, whether registered or not, applications to register and registrations of the same and like protections, and the entire goodwill of the business of Grantor connected with and symbolized by such trademarks, including without limitation those set forth on Exhibit C attached hereto (collectively, the “Trademarks”);

(f) All mask works or similar rights available for the protection of semiconductor chips, now owned or hereafter acquired, including, without limitation those set forth on Exhibit D attached hereto (collectively, the “Mask Works”);

(g) Any and all claims for damages by way of past, present and future infringements of any of the rights included above, with the right, but not the obligation, to sue for and collect such damages for said use or infringement of the intellectual property rights identified above;

(h) All licenses or other rights to use any of the Copyrights, Patents, Trademarks, or Mask Works and all license fees and royalties arising from such use to the extent permitted by such license or rights;

(i) All amendments, extensions, renewals and extensions of any of the Copyrights, Trademarks, Patents, or Mask Works; and

(j) All proceeds and products of the foregoing, including without limitation all payments under insurance or any indemnity or warranty payable in respect of any of the foregoing.

2. Recordation. Grantor authorizes the Commissioner for Patents, the Commissioner for Trademarks and the Register of Copyrights and any other government officials to record and register this Agreement upon request by Bank.

3. Authorization. Grantor hereby authorizes Bank to (a) modify this Agreement unilaterally by amending the exhibits to this Agreement to include any Intellectual Property Collateral which Grantor obtains subsequent to the date of this Agreement, and (b) file a duplicate original of this Agreement containing amended exhibits reflecting such new Intellectual Property Collateral.

4. Loan Documents. This Agreement has been entered into pursuant to and in conjunction with the Loan Agreement, which is hereby incorporated by reference. The provisions of the Loan Agreement shall supersede and control over any conflicting or inconsistent provision herein. The rights and remedies of Bank with respect to the Intellectual Property Collateral are as provided by the Loan Agreement and related documents, and nothing in this Agreement shall be deemed to limit such rights and remedies.

5. Execution in Counterparts. This Agreement may be executed in counterparts (and by different parties hereto in different counterparts), each of which shall constitute an original, but all of which when taken together shall constitute a single contract. Delivery of an executed counterpart of a signature page to this Agreement by facsimile or in electronic (i.e., “pdf” or “tif” format) shall be effective as delivery of a manually executed counterpart of this Agreement.

6. Successors and Assigns. This Agreement will be binding on and shall inure to the benefit of the parties hereto and their respective successors and assigns.

7. Governing Law. California law governs this Agreement without regard to principles of conflicts of law.

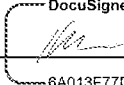
IN WITNESS WHEREOF, the parties have caused this Intellectual Property Security Agreement to be duly executed by its officers thereunto duly authorized as of the first date written above.

GRANTOR:

Address:

15500 Wells Port Drive
Austin, TX 78728
Attn: Hollie Osbourn, CFO and Treasurer

HART INTERCIVIC, INC.

By:  DocuSigned by:
6A013F77D14D40D...
Name: Hollie Osbourn

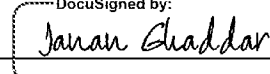
Title: Chief Financial Officer and Treasurer

BANK:

Address:

504 Lavaca Street, Suite 1100
Austin, TX 78701
Attn: Janan Ghaddar, Vice President

SILICON VALLEY BANK

By:  DocuSigned by:
13D38F0690F3448...
Name: Janan Ghaddar

Title: Vice President

[Signature Page to Intellectual Property Security Agreement]

EXHIBIT A

Copyrights

<u>Description</u>	Registration/ Application <u>Number</u>	Registration/ Application <u>Date</u>
Ballot Now	TX0005787201	4/19/02
Boss	TX0005787200	4/19/02
eSlate firmwave	TX0005598239	4/19/02
JBC firmwave	TX0005787199	4/19/02
SERVO	TX0005672241	4/19/02
Tally	TX0005786099	4/19/02

EXHIBIT B

Patents

<u>Description</u>	<u>Registration/ Application Number</u>	<u>Registration/ Application Date</u>
Portable voting booth	6827262	12/7/04
Distributed network voting system	6873966	3/29/05
Precinct voting system	7032821	4/25/06
Automated processing of by-mail ballots	7216807	5/15/07
Landing lights for multi-purpose configurable voting system	8985435	3/24/15
Multi-purpose configurable voting system	13967054	8/14/13
System and Method for Identifying and Exporting Cast Vote Record Data	14817317	8/4/2015
System and Method for Transmission And Display Of Election Voting Data	15242784	8/22/2016
System and Method for Identifying and Recovering Stranded Voting Ballots	10505801	12/10/19
System and Method for Electronic Voting Network Having Physical Port Blockers	10438433	10/8/19
Election Voting Network Graphical User Interface	823336	7/17/18
Election Voting Network Graphical User Interface	29653559	6/15/18
Haptic Feedback Apparatus And Methods For An Election Voting Systems	10169943	1/1/19
Election Voting System Printed Vote Records	16517011	7/19/19
Optical Character Recognition of Voter Selections for Cast Vote Records	10445966	10/15/19
Optical Character Recognition of Voter Selections for Cast Vote Records	10573111	2/25/20
Optical Character Recognition of Voter Selections for Cast Vote Records	16745621	1/17/20
Method And Apparatus For Transportable And Useable Voting Equipment to Provide Curbside Voting And Printing Of Printed Vote Records	62932554	11/8/19

EXHIBIT C

Trademarks

<u>Description</u>	<u>Registration/ Application Number</u>	<u>Registration/ Application Date</u>
HART INTERCIVIC	3255209	6/26/07
VBO	3613926	4/28/09
VERITY	4773254	7/14/15
BALLOT NOW	2837160	4/27/04
H	2906270	11/30/04
ESLATE	2978082	7/26/05
ESLATE	3058690	2/14/06
HART INTERCIVIC	3305756	10/9/07

EXHIBIT D

Mask Works

<u>Description</u>	Registration/ Application <u>Number</u>	Registration/ Application <u>Date</u>
None		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		16745621
	Filing Date		2020-01-17
	First Named Inventor	JAMES M. CANTER	
	Art Unit		
	Examiner Name		
	Attorney Docket Number		HART:032C2

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

Add

U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

Add

FOREIGN PATENT DOCUMENTS							Remove	
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²ⁱ	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button

Add

NON-PATENT LITERATURE DOCUMENTS			Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number		16745621
Filing Date		2020-01-17
First Named Inventor	JAMES M. CANTER	
Art Unit		
Examiner Name		
Attorney Docket Number	HART:032C2	

1	Election Systems & Software, LLC. v. Hart Intercivic, Inc., "Petitioner's Reply To Patent Owner's Response", Patent No. 10,445,966, February 17, 2021, 38 pgs.
2	Election Systems & Software, LLC. v. Hart Intercivic, Inc., "Video Conference Deposition Of Daniel P. Lopresti, Ph.D.", Patent No. 10,445,966, February 5, 2021, 87 pgs.
3	Federal Information Processing Standards Publication, "Digital Signature Standard (DSS)", Information Technology Laboratory, FIPS PUB 186-4, July 2013, 130 pgs.
4	Election Systems & Software, LLC. v. Hart Intercivic, Inc., "Supplemental Declaration Of Michael I. Shamos, Ph.D., J. D.", Patent No. 10,445,966, February 17, 2021, 34 pgs.
5	Esakov et al., "Issues In Automatic OCR Error Classification", Panasonic Technologies, Inc., December 31, 1994, 12 pgs.
6	Damerau, "A Technique For Computer Detection And Correction Of Spelling Errors", Communications Of The ACM, Vol. 7, No. 3, March 1964, 6 pgs. :
7	Seni et al., "Generalizing Edit Distance To Incorporate Domain Information: Handwritten Text Recognition As A Case Study", Pattern Recognition, Vol. 29, No. 3, 1996, 10 pgs.

If you wish to add additional non-patent literature document citation information please click the Add button

Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16745621
Filing Date	2020-01-17
First Named Inventor	JAMES M. CANTER
Art Unit	
Examiner Name	
Attorney Docket Number	HART:032C2

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☒ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Richard D. Egan/	Date (YYYY-MM-DD)	2021-02-25
Name/Print	Richard D. Egan	Registration Number	36788

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	42021716
Application Number:	16745621
International Application Number:	
Confirmation Number:	6960
Title of Invention:	OPTICAL CHARACTER RECOGNITION OF VOTER SELECTIONS FOR CAST VOTE RECORDS
First Named Inventor/Applicant Name:	James M. Canter
Customer Number:	36275
Filer:	Richard D. Egan/Marty Jones
Filer Authorized By:	Richard D. Egan
Attorney Docket Number:	HART:032C2
Receipt Date:	25-FEB-2021
Filing Date:	17-JAN-2020
Time Stamp:	13:20:52
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	IDS.pdf	1035651	no	4
			55369b3483b38f1d47769fe4e22b7ea91469e36a		

Warnings:

Information:					
A U.S. Patent Number Citation or a U.S. Publication Number Citation is required in the Information Disclosure Statement (IDS) form for autoloading of data into USPTO systems. You may remove the form to add the required data in order to correct the Informational Message if you are citing U.S. References. If you chose not to include U.S. References, the image of the form will be processed and be made available within the Image File Wrapper (IFW) system. However, no data will be extracted from this form. Any additional data such as Foreign Patent Documents or Non Patent Literature will be manually reviewed and keyed into USPTO systems.					
2	Non Patent Literature	C2.pdf	1425057	no	87
			5c2d82f51e417bacc6033114cadf3952b6bd7145		
Warnings:					
Information:					
3	Non Patent Literature	C5.pdf	2639641	no	12
			62156e802f0b5e094c6207681feed9ea1b3206bf		
Warnings:					
Information:					
4	Non Patent Literature	C6.pdf	1283412	no	6
			1f0d11baa6539d4c0c881497a754b61834fa5fc1		
Warnings:					
Information:					
5	Non Patent Literature	C7.pdf	1491165	no	10
			0b51bb6bdb9c1a978894bd6efe0b351fee2a23d7		
Warnings:					
Information:					
6	Non Patent Literature	C1.pdf	495508	no	38
			421fe832d143429fad41d94e90aac8d838131dc		
Warnings:					
Information:					
7	Non Patent Literature	C3.pdf	837238	no	130
			c3b899f011d80c9604b74b5f884fac69f15a29d		
Warnings:					
Information:					

8	Non Patent Literature	C4.pdf	<div>314486</div> <div>de8633508026d94d819fo0d7352e68eb4f1d37f6</div>	no	34
Warnings:					
Information:					
Total Files Size (in bytes):			9522158		
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/745,621	03/16/2021	10950078	HART:032C2	6960

36275 7590 02/24/2021
Egan, Peterman, Enders & Huston LLP.
1101 S. Capital of Texas Highway
Bldg C, Suite 200
Austin, TX 78746

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (application filed on or after May 29, 2000)

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (<http://pair.uspto.gov>).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site <http://pair.uspto.gov> for additional applicants):

Hart InterCivic, Inc., Austin, TX;
James M. Canter, Austin, TX;
Drew E. Tinney, Austin, TX;
Ievgen Konovalenko, Austin, TX;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (03-15)

Approved for use through 07/31/2016, OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		16745621	
	Filing Date		2020-01-17	
	First Named Inventor	JAMES M. CANTER		
	Art Unit			
	Examiner Name			
	Attorney Docket Number	HART:032C2		

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS						
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS								
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16745621
Filing Date	2020-01-17
First Named Inventor	JAMES M. CANTER
Art Unit	
Examiner Name	
Attorney Docket Number	HART:032C2

/L.A.G/	1	Certified Translation of Brazil Patent Document BR-102013018558-2 A2, Nadaf, "Verification Ballot Printing And Collection Equipment And Equipment For Auditing And Counting Votes Printed On Verification Ballots For A Mechatronic Voting Model", Filed July 19, 2013, 158 pgs.	☐
If you wish to add additional non-patent literature document citation information please click the Add button			
EXAMINER SIGNATURE			
Examiner Signature	/LAURA A GUDORF/	Date Considered	02/05/2021
*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.			
<p>¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.</p>			

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16745621
Filing Date	2020-01-17
First Named Inventor	JAMES M. CANTER
Art Unit	
Examiner Name	
Attorney Docket Number	HART:032C2

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

- ☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

- ☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

- ☒ See attached certification statement.
- ☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.
- ☐ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Richard D. Egan/	Date (YYYY-MM-DD)	2021-02-01
Name/Print	Richard D. Egan	Registration Number	36788

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: JAMES M. CANTER

Filed: JANUARY 17, 2020

For: OPTICAL CHARACTER RECOGNITION OF VOTER SELECTIONS
FOR CAST VOTE RECORDS

Serial No.: 16/745,621

Group Art Unit: 2876

Examiner: GUDORF, L.

Atty Docket No.: HART:032C2

Electronic Filed

**CERTIFICATION STATEMENT OF SUPPLEMENTAL INFORMATION DISCLOSURE
STATEMENT**Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313

Sir:

This Information Disclosure Statement resubmits a reference that has already been submitted and considered by the Patent Examiner. The Reference was previously submitted as a "Foreign Patent Document" in a prior Information Disclosure Statement. The prior submission includes the translation, translator's certification and the actual Brazilian document. The Brazilian document was also previously submitted as a stand-alone document in an Information Disclosure Statement. Because the translation document includes the translation materials in addition to the foreign patent document materials, the reference is being resubmitted under the "Non-Patent Literature Documents" out of an abundance of caution and entitled "Certified Translation of Brazil Patent Document BR102013018558-2 A2.

Applicant respectfully requests that the listed documents be made of record in the present case.

Respectfully submitted,

/Richard D. Egan/

Richard D. Egan

Reg. No. .36,788

Attorney for Applicant

EGAN, ENDERS & HUSTON, LLP
1101 South Capital of Texas Highway
Building C, Suite 200
Austin, Texas 78746
(512) 347-1611
FAX: (512) 347-1615

Enclosures

Document Description: Issue Fee Payment (PTO-85B)

Issue Fee Transmittal Form

Application Number	Filing Date	First Named Inventor	Atty. Docket No.	Confirmation No.
16745621	17-Jan-2020	James Canter	HART:032C2	6960

TITLE OF INVENTION :

OPTICAL CHARACTER RECOGNITION OF VOTER SELECTIONS FOR CAST VOTE RECORDS

Entity Status	Application Type	Art Unit	Class - Subclass	EXAMINER
Regular Undiscounted	Utility under 35 USC 111(a)	2876	386000	LAURA GUDORF
Issue Fee Due	Publication Due	Total Fee(s) Due	Date Due	Prev. Paid Fee
\$1200	\$0	\$1200	22-Apr-2021	\$0

1.Change of Correspondence Address and/or Indication Of Fee Address (37 CFR 1.33 & 1.363)

Current Correspondence Address:	Current Indicated Fee Address :
36275 Egan, Peterman, Enders & Huston LLP. 1101 S. Capital of Texas Highway Bldg C, Suite 200 Austin TX 78746 UNITED STATES 512-347-1611 epehadmin@ipaustin.com	
☐ Change of correspondence address requested, system generated AIA/122-EFS form attached	☐ Fee Address indication requested, system generated SB/47-EFS form attached

2.Entity Status**Change in Entity Status**

Applicant certifying micro entity status; system generated Micro Entity certification form attached. See 37 CFR 1.29.

Note: Absent a valid certification of micro entity status, issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
 If this box is checked, you will be prompted to choose a micro entity status on the gross income basis (37 CFR 1.29(a)) or the institution of higher education basis (37 CFR 1.29(d)), and make the applicable certification online.



Applicant asserting small entity status. See 37 CFR 1.27.

Note: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.



Applicant changing to regular undiscounted fee status.

Note: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.



Document Description: Issue Fee Payment (PTO-85B)

3.The Following Fee(s) Are Submitted:

☒ Issue Fee

☐ I authorize USPTO to apply my previously paid issue fee to the current fees due

☐ Publication Fee

☐ The Director is hereby authorized to apply my previously paid issue fee to the current fee due and to charge deficient fees to Deposit Account Number _____

☐ Advance Order - # of copies _____

☒ If in **addition** to the payment of the issue fee amount submitted with this form, there are any discrepancies in any amount(s) due, the Director is authorized to charge any deficiency, or credit any overpayment, to Deposit Account Number 101205.
The **issue fee must be submitted** with this form. **If payment of the issue fee does not accompany this form, checking this box and providing a deposit account number will NOT be effective to satisfy full payment of the fee(s) due.**

4.Firm and/or Attorney Names To Be Printed

NOTE: If no name is listed, no name will be printed
For printing on the patent front page, list to be displayed as entered

1. Egan Peterman Enders Huston
2.
3.

5.Assignee Name(s) and Residence Data To Be Printed

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

Name	City	State	Country	Category
Hart InterCivic, Inc.	Austin	TEXAS	united states	corporation

6.Signature

I certify, in accordance with 37 CFR 1.4(d)(4) that I am an attorney or agent registered to practice before the Patent and Trademark Office who has filed and has been granted power of attorney in this application. I also certify that this Fee(s) Transmittal form is being transmitted to the USPTO via EFS-WEB on the date indicated below.

Signature	/Richard D. Egan/	Date	02-04-2021
Name	Richard D. Egan	Registration Number	36788

Electronic Patent Application Fee Transmittal

Application Number:	16745621			
Filing Date:	17-Jan-2020			
Title of Invention:	OPTICAL CHARACTER RECOGNITION OF VOTER SELECTIONS FOR CAST VOTE RECORDS			
First Named Inventor/Applicant Name:	James M. Canter			
Filer:	Richard D. Egan/Marty Jones			
Attorney Docket Number:	HART:032C2			
Filed as Large Entity				
Filing Fees for Utility under 35 USC 111(a)				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
UTILITY APPL ISSUE FEE	1501	1	1200	1200
PUBL. FEE- EARLY, VOLUNTARY, OR NORMAL	1504	1	0	0
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				1200

Electronic Acknowledgement Receipt

EFS ID:	41837375
Application Number:	16745621
International Application Number:	
Confirmation Number:	6960
Title of Invention:	OPTICAL CHARACTER RECOGNITION OF VOTER SELECTIONS FOR CAST VOTE RECORDS
First Named Inventor/Applicant Name:	James M. Canter
Customer Number:	36275
Filer:	Richard D. Egan/Marty Jones
Filer Authorized By:	Richard D. Egan
Attorney Docket Number:	HART:032C2
Receipt Date:	04-FEB-2021
Filing Date:	17-JAN-2020
Time Stamp:	14:06:40
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	\$ 1200
RAM confirmation Number	E202124E06354020
Deposit Account	101205
Authorized User	Marty Jones

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

Ex. 2007 / PGR2025-00066 / Page 28 of 557

Election Systems & Software, LLC v. Hart Intercivic, Inc.

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	Web85b.pdf	46270	no	2
			7a33230f19cd197dc5cd969cd2bd21efeabf10a6		
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	31832	no	2
			16a1689aaa488a699cf45ec8405bf33912dc470		
Warnings:					
Information:					
Total Files Size (in bytes):			78102		
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		16745621
	Filing Date		2020-01-17
	First Named Inventor	JAMES M. CANTER	
	Art Unit		
	Examiner Name		
	Attorney Docket Number	HART:032C2	

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS						
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS								
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16745621
Filing Date	2020-01-17
First Named Inventor	JAMES M. CANTER
Art Unit	
Examiner Name	
Attorney Docket Number	HART:032C2

1	Certified Translation of Brazil Patent Document BR-102013018558-2 A2, Nadaf, "Verification Ballot Printing And Collection Equipment And Equipment For Auditing And Counting Votes Printed On Verification Ballots For A Mechatronic Voting Model", Filed July 19, 2013, 158 pgs.	☐
---	--	--------------------------

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16745621
Filing Date	2020-01-17
First Named Inventor	JAMES M. CANTER
Art Unit	
Examiner Name	
Attorney Docket Number	HART:032C2

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

- ☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

- ☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

- ☒ See attached certification statement.
- ☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.
- ☐ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Richard D. Egan/	Date (YYYY-MM-DD)	2021-02-01
Name/Print	Richard D. Egan	Registration Number	36788

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: JAMES M. CANTER

Filed: JANUARY 17, 2020

For: OPTICAL CHARACTER RECOGNITION OF VOTER SELECTIONS
FOR CAST VOTE RECORDS

Serial No.: 16/745,621

Group Art Unit: 2876

Examiner: GUDORF, L.

Atty Docket No.: HART:032C2

Electronic Filed

**CERTIFICATION STATEMENT OF SUPPLEMENTAL INFORMATION DISCLOSURE
STATEMENT**

Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313

Sir:

This Information Disclosure Statement resubmits a reference that has already been submitted and considered by the Patent Examiner. The Reference was previously submitted as a “Foreign Patent Document” in a prior Information Disclosure Statement. The prior submission includes the translation, translator’s certification and the actual Brazilian document. The Brazilian document was also previously submitted as a stand-alone document in an Information Disclosure Statement. Because the translation document includes the translation materials in addition to the foreign patent document materials, the reference is being resubmitted under the “Non-Patent Literature Documents” out of an abundance of caution and entitled “Certified Translation of Brazil Patent Document BR102013018558-2 A2.

Applicant respectfully requests that the listed documents be made of record in the present case.

Respectfully submitted,

/Richard D. Egan/

Richard D. Egan

Reg. No. .36,788

Attorney for Applicant

EGAN, ENDERS & HUSTON, LLP
1101 South Capital of Texas Highway
Building C, Suite 200
Austin, Texas 78746
(512) 347-1611
FAX: (512) 347-1615

Enclosures

Electronic Patent Application Fee Transmittal

Application Number:	16745621			
Filing Date:	17-Jan-2020			
Title of Invention:	OPTICAL CHARACTER RECOGNITION OF VOTER SELECTIONS FOR CAST VOTE RECORDS			
First Named Inventor/Applicant Name:	James M. Canter			
Filer:	Richard D. Egan/Marty Jones			
Attorney Docket Number:	HART:032C2			
Filed as Large Entity				
Filing Fees for Utility under 35 USC 111(a)				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
SUBMISSION- INFORMATION DISCLOSURE STMT	1806	1	260	260
Total in USD (\$)				260

Electronic Acknowledgement Receipt

EFS ID:	41800139
Application Number:	16745621
International Application Number:	
Confirmation Number:	6960
Title of Invention:	OPTICAL CHARACTER RECOGNITION OF VOTER SELECTIONS FOR CAST VOTE RECORDS
First Named Inventor/Applicant Name:	James M. Canter
Customer Number:	36275
Filer:	Richard D. Egan/Marty Jones
Filer Authorized By:	Richard D. Egan
Attorney Docket Number:	HART:032C2
Receipt Date:	01-FEB-2021
Filing Date:	17-JAN-2020
Time Stamp:	14:25:30
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	\$260
RAM confirmation Number	E202121E25530463
Deposit Account	101205
Authorized User	Marty Jones

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

37 CFR 1.16 (National application filing, search, and examination fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

Ex. 2007 / PGR2025-00066 / Page 38 of 557

Election Systems & Software, LLC v. Hart Intercivic, Inc.

37 CFR 1.19 (Document supply fees)
37 CFR 1.20 (Post Issuance fees)
37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	IDS.pdf	348533	no	6
			718f14c856be07a0bc8b2f5c072711125c795a8d		

Warnings:

Information:

This is not an USPTO supplied IDS fillable form

2	Non Patent Literature	C1.pdf	25265615	no	158
			dd4e74ac157cd3d8b3213d56ab0f1d64cbca65d0		

Warnings:

Information:

3	Fee Worksheet (SB06)	fee-info.pdf	30502	no	2
			ddba3d52be32ee6d587fe702ba57b675a140f6e4		

Warnings:

Information:

Total Files Size (in bytes):	25644650
-------------------------------------	----------

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

36275 7590 01/22/2021
Egan, Peterman, Enders & Huston LLP.
1101 S. Capital of Texas Highway
Bldg C, Suite 200
Austin, TX 78746

EXAMINER	
GUDORF, LAURA A	
ART UNIT	PAPER NUMBER

2876

DATE MAILED: 01/22/2021

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/745,621	01/17/2020	James M. Canter	HART:032C2	6960

TITLE OF INVENTION: OPTICAL CHARACTER RECOGNITION OF VOTER SELECTIONS FOR CAST VOTE RECORDS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	\$1200	\$0.00	\$0.00	\$1200	04/22/2021

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

36275 7590 01/22/2021
Egan, Peterman, Enders & Huston LLP.
1101 S. Capital of Texas Highway
Bldg C, Suite 200
Austin, TX 78746

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/745,621	01/17/2020	James M. Canter	HART:032C2	6960

TITLE OF INVENTION: OPTICAL CHARACTER RECOGNITION OF VOTER SELECTIONS FOR CAST VOTE RECORDS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	\$1200	\$0.00	\$0.00	\$1200	04/22/2021

EXAMINER	ART UNIT	CLASS-SUBCLASS
GUDORF, LAURA A	2876	235-386000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,

1 _____

(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

2 _____

3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. Fees submitted: ☐ Issue Fee ☐ Publication Fee (if required) ☐ Advance Order - # of Copies _____

4b. Method of Payment: (Please first reapply any previously paid fee shown above)

☐ Electronic Payment via EFS-Web ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)

☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. Change in Entity Status (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29

☐ Applicant asserting small entity status. See 37 CFR 1.27

☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____

Date _____

Typed or printed name _____

Registration No. _____

Ex. 2007 / PGR2025-00066 / Page 41 of 557



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/745,621	01/17/2020	James M. Canter	HART:032C2	6960
36275	7590	01/22/2021	EXAMINER	
Egan, Peterman, Enders & Huston LLP. 1101 S. Capital of Texas Highway Bldg C, Suite 200 Austin, TX 78746			GUDORF, LAURA A	
			ART UNIT	PAPER NUMBER
			2876	

DATE MAILED: 01/22/2021

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 16/745,621	Applicant(s) Canter et al.	
	Examiner LAURA A GUDORF	Art Unit 2876	AIA (FITF) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to applicant submission filed 12/22/2020.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☒ The allowed claim(s) is/are 1-24. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a) ☐ All b) ☐ Some *c) ☐ None of the:

1. ☐ Certified copies of the priority documents have been received.

2. ☐ Certified copies of the priority documents have been received in Application No. _____.

3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892) 2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date <u>11/30/2020</u> . 3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____. 4. ☐ Interview Summary (PTO-413), Paper No./Mail Date. _____.	5. ☐ Examiner's Amendment/Comment 6. ☒ Examiner's Statement of Reasons for Allowance 7. ☐ Other _____.
--	--

/ LAURA A GUDORF/
Primary Examiner, Art Unit 2876

DETAILED ACTION

Summary

This Office Action is responsive to Applicant submission filed 12/22/2020.

Response to Arguments

Applicant's arguments, see pages 8-21, filed 12/22/2020, with respect to the 102(a)(1)/102(a)(2) rejection of claims 1-22 have been fully considered and are persuasive. The rejection of claims 1-22 has been withdrawn.

Allowable Subject Matter

Claims 1-24 are allowed.

The following is an examiner's statement of reasons for allowance:

Regarding independent claim 1:

The prior art of record fails to teach or fairly suggest, either singularly or in combination thereof, a method for electronic voting using printed vote records comprising each and every one of the following limitations (*emphasis added*):

Generating a printed vote record of at least one vote selection of a voter;

Providing, on the printed vote record, voter readable text indicating the voter's at least one vote selection;

Providing, on the printed vote record, encoded data, the encoded data based at least in part on the voter's at least one vote selection;

Electronically scanning the voter readable text on the printed vote record to create a first data set, the first data set based at least in part on the voter's at least one vote selection;

Electronically scanning the encoded data on the printed vote record to create a second data set, the second data set based at least in part on the voter's at least one vote selection;

Comparing the first data set and the second data set; and

Generating a cast vote record indicating the voter's at least one vote selection, wherein, prior to generating the cast vote record, confirming an accuracy of one or more voter selections to be cast based at least in part on a comparison of the first data set and the second data set.

Claims 2-24 depend from independent claim 1 and are therefore allowed.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LAURA A GUDORF whose telephone number is (571)270-7607. If the Examiner cannot be reached by telephone, she can be reached through the following e-mail address: laura.gudorf@uspto.gov. The examiner can normally be reached on M-F 6:00-4:00 PM.

If attempts to reach the examiner by telephone and e-mail are unsuccessful, the examiner's supervisor, Michael Lee can be reached on (571)272-2398. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

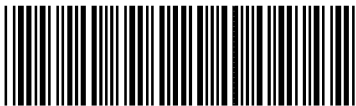
Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/LAURA A GUDORF/
Primary Examiner, Art Unit 2876

<i>Index of Claims</i> 	Application/Control No. 16/745,621	Applicant(s)/Patent Under Reexamination Canter et al.
	Examiner LAURA A GUDORF	Art Unit 2876

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS										
☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47										
CLAIM		DATE								
Final	Original	09/29/2020	01/13/2021							
	1	✓	=							
	2	✓	=							
	3	✓	=							
	4	✓	=							
	5	✓	=							
	6	✓	=							
	7	✓	=							
	8	✓	=							
	9	✓	=							
	10	✓	=							
	11	✓	=							
	12	✓	=							
	13	✓	=							
	14	✓	=							
	15	✓	=							
	16	✓	=							
	17	✓	=							
	18	✓	=							
	19	✓	=							
	20	✓	=							
	21	✓	=							
	22	✓	=							
	23		=							
	24		=							

<i>Search Notes</i> 	Application/Control No. 16/745,621	Applicant(s)/Patent Under Reexamination Canter et al.
	Examiner LAURA A GUDORF	Art Unit 2876

CPC - Searched*		
Symbol	Date	Examiner
G07C13/00; G06K7/10346; G06K9/00442; G06K17/0032	09/22/2020	LAG

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

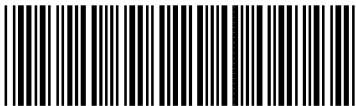
US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
Inventor name search	09/22/2020	LAG
EAST - see attached search history	09/22/2020	LAG
PGR2020-00031 Reviewed Petition for Post Grant Review of U.S. Patent 10,445,966 on 09/21/2020	09/22/2020	LAG
Updated EAST search - see attached for details	01/13/2021	LAG

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
G07C	13/00	01/13/2021	LAG
G06K	7/10346; 9/00442; 17/0032	01/13/2021	LAG

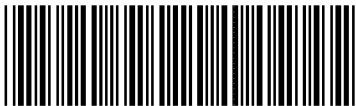
	Ex. 2007 / PGR2025-00066 / Page 49 of 557
--	---

Issue Classification 	Application/Control No. 16/745,621	Applicant(s)/Patent Under Reexamination Canter et al.
	Examiner LAURA A GUDORF	Art Unit 2876

CPC						
Symbol					Type	Version
G07C	/	13	/	00	F	2013-01-01
G06K	/	17	/	0032	I	2013-01-01
G06K	/	9	/	00442	I	2013-01-01
G06K	/	7	/	10346	I	2013-01-01
G06K	/	2209	/	01	A	2013-01-01

CPC Combination Sets					
Symbol			Type	Set	Ranking
/	/	/			

NONE (Assistant Examiner) _____ (Date) _____		Total Claims Allowed: 24	
/LAURA A GUDORF/ Primary Examiner, Art Unit 2876 (Primary Examiner) _____ (Date) 13 January 2021		O.G. Print Claim(s) 1	O.G. Print Figure 2

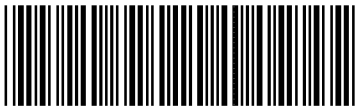
Issue Classification 	Application/Control No. 16/745,621	Applicant(s)/Patent Under Reexamination Canter et al.
	Examiner LAURA A GUDORF	Art Unit 2876

INTERNATIONAL CLASSIFICATION			
CLAIMED			
G07C13/00	/	13	/ 00
G06K17/00	/	17	/ 00
G06K9/00	/	9	/ 00
G06K7/10	/	7	/ 10
NON-CLAIMED			
	/		/

US ORIGINAL CLASSIFICATION	
CLASS	SUBCLASS
235	386

CROSS REFERENCES(S)						
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)					

NONE (Assistant Examiner) _____ (Date) _____		Total Claims Allowed: 24	
/LAURA A GUDORF/ Primary Examiner, Art Unit 2876 (Primary Examiner) _____ (Date) _____		13 January 2021 O.G. Print Claim(s) 1	O.G. Print Figure 2

Issue Classification 	Application/Control No. 16/745,621	Applicant(s)/Patent Under Reexamination Canter et al.
	Examiner LAURA A GUDORF	Art Unit 2876

☒ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47															
CLAIMS															
Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
	1		10		19										
	2		11		20										
	3		12		21										
	4		13		22										
	5		14		23										
	6		15		24										
	7		16												
	8		17												
	9		18												

NONE (Assistant Examiner) _____ (Date) _____		Total Claims Allowed: 24	
/LAURA A GUDORF/ Primary Examiner, Art Unit 2876 (Primary Examiner) _____ (Date) 13 January 2021		O.G. Print Claim(s) 1	O.G. Print Figure 2

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	33,569	G07C13/00.cpc. G06K7/10346.cpc. G06K7/10346.cpc. G06K17/0032.cpc. G06K2209/01.cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2021/01/13 06:35
L2	9,543	L1 and (OCR (optical near2 (recognition read\$3)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2021/01/13 06:36
L3	851	L2 and (vote\$1 voting)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2021/01/13 06:43
L4	163	L3 and (confirm\$5 with (vote\$1 selection\$1 choice\$1))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2021/01/13 07:28

1/13/2021 9:04:23 AM

C:\Users\lgudorf\Documents\EAST\Workspaces\16745621.wsp

Bibliographic Data

Application No: 16/745,621

Foreign Priority claimed: ☐ Yes ☒ No

35 USC 119 (a-d) conditions met: ☐ Yes ☒ No ☐ Met After Allowance

Verified and Acknowledged: /LAURA A GUDORF/

Examiner's Signature

Initials

Title:

Optical Character Recognition Of Voter Selections For Cast Vote Records

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
01/17/2020	235	2876	HART:032C2
RULE			

APPLICANTS

Hart InterCivic, Inc., Austin, TX, UNITED STATES

INVENTORS

James M. Canter, Austin, TX, UNITED STATES

Drew E. Tinney, Austin, TX, UNITED STATES

Ievgen Konovalenko, Austin, TX, UNITED STATES

CONTINUING DATA

This application is a CON of 16560222 09/04/2019 PAT 10573111

16560222 is a CON of 16239607 01/04/2019 PAT 10445966

16239607 has PRO of 62711212 07/27/2018

FOREIGN APPLICATIONS

IF REQUIRED, FOREIGN LICENSE GRANTED**

02/04/2020

STATE OR COUNTRY

UNITED STATES

ADDRESS

Egan, Peterman, Enders & Huston LLP.

1101 S. Capital of Texas Highway

Bldg C, Suite 200

Austin, TX 78746

UNITED STATES

FILING FEE RECEIVED

\$1,920

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (03-15)

Approved for use through 07/31/2016. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)

Application Number	16745621
Filing Date	2020-01-17
First Named Inventor	JAMES M. CANTER
Art Unit	
Examiner Name	
Attorney Docket Number	HART:032C2

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

Add

U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/L.A.G/	1	20060282442		2006-12-14	Lennon et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button.

Add

FOREIGN PATENT DOCUMENTS								<div>Remove</div>
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²ⁱ	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button

Add

NON-PATENT LITERATURE DOCUMENTS						Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.				T ⁵

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16745621	
Filing Date	2020-01-17	
First Named Inventor	JAMES M. CANTER	
Art Unit		
Examiner Name		
Attorney Docket Number	HART:032C2	

1	
---	--

If you wish to add additional non-patent literature document citation information please click the Add button

Add

EXAMINER SIGNATURE

Examiner Signature	/LAURA A GUDORF/	Date Considered	01/08/2021
--------------------	------------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	16745621		
Filing Date	2020-01-17		
First Named Inventor	JAMES M. CANTER		
Art Unit			
Examiner Name			
Attorney Docket Number	HART:032C2		

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Richard D. Egan/	Date (YYYY-MM-DD)	2020-11-30
Name/Print	Richard D. Egan	Registration Number	36788

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

April 9, 2019

By Email & Hand Delivery

The Honorable Amy Klobuchar
425 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Gary C. Peters
724 Hart Senate Office Building
Washington, DC 20510

The Honorable Jack Reed
728 Hart Senate Office Building
Washington, DC 20510

The Honorable Mark R. Warner
703 Hart Senate Office Building
Washington, DC 20510

Dear Senators Klobuchar, Peters, Reed, and Warner:

Thank you for your letter of March 26, 2019, and for the opportunity to discuss how Election Systems & Software (ES&S) is working with many stakeholders, including the U.S. government, to secure and ensure faith in our system of democracy.

Please find below the answers to your questions.

- 1. What specific steps are you taking to strengthen election security ahead of 2020? How can Congress and the federal government support these actions?*

We appreciate the question regarding the role of ES&S, Congress, and the federal government in supporting and strengthening the integrity of elections. At the outset, we want to be clear that *ES&S fully supports the use of paper ballots and post-election audits as a way to ensure accuracy and increase confidence in our country's election process.*

In regard to ES&S' work to strengthen election security ahead of 2020:

1. Testing: As standard procedure, our internal security team conducts thorough and pervasive penetration testing of our hardware and software using the same modern security tools that hackers might use to make sure our equipment is secure before it ever reaches the customer. After the 2016 election, to complement our own testing, we submitted our current hardware to third-party security research firms to independently verify the security of our devices. In addition, ES&S recently submitted its full end-to-end voting configuration of software and hardware for testing by the Idaho National Laboratory (INL), the nation's leading center for research and development in energy, national security, science and environment, to perform third-party independent testing of both our hardware and software to ensure the resilience and security of our voting systems.

Maintain Voter Confidence. Enhance the Voting Experience.

2. Coordination: In strategic partnerships, ES&S met with the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) leadership frequently over the past year, and we signed up for DHS weekly cyber-hygiene scans of our external web presence. ES&S has joined both the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) and the Information Technology Information Sharing and Analysis Center (IT-ISAC) to take advantage of the significant cyber threat sharing channels these groups support, and we have requested and installed Albert sensors in our hosted voter registration environments in order to detect and thwart any potential indicators of compromise. Albert is a unique network security monitoring solution that provides continuous remote monitoring and delivery of automated alerts on both traditional and advanced network threats for state and local jurisdictions, allowing election jurisdictions and ES&S to respond quickly when data may be at risk. Combined with an in-depth review conducted by expert analysts through the Center for Internet Security's (CIS) 24/7 Security Operations Center, Albert is a fully monitored and managed service which complements ES&S' existing, robust suite of cybersecurity controls.
3. Education: ES&S has conducted numerous election security training sessions, presentations, and discussions for state and local election officials who use our equipment to continue to educate and inform them of best practices for securing election equipment and processes.
4. Additional security: ES&S has implemented additional security controls protecting our corporate network environment, including independent vulnerability assessments and DMARC email security to further strengthen our corporate network from cyber threats. All ES&S personnel (employees, contractors, temps, and interns) are required to carry a security badge that limits access to only the areas required to perform their specific job function. All building entrances, elevators, and sensitive internal areas of ES&S facilities are covered by electronic door badge access and security cameras. Our physical security posture has been reviewed by the local office of the DHS Critical Infrastructure Physical Security Specialist for this area of the nation. ES&S conducts on-site reviews of our vendor partners' physical and information security programs to ensure they are also following industry best practices to secure their facilities and environments.

Regarding Congressional support, we support Congress adopting legislation to establish a program mandating that all voting machine suppliers submit their systems to stronger, programmatic security testing conducted by vetted and approved researchers. We also believe Congress should mandate physical paper records of votes to enable an effective, meaningful audit of each voter's selections. Mandating the use of a physical paper record sets the stage for all jurisdictions to perform statistically valid post-election audits. As noted above, *ES&S fully supports the use of paper ballots and post-election audits as a way to ensure accuracy and increase confidence in our country's election process.*

2. *What additional information is necessary regarding VVSG 2.0 in order for your companies to begin developing systems that comply with the new guidelines?*

ES&S looks forward to the approval of the VVSG 2.0, so that we can work to ensure our solutions meet or exceed these guidelines. ES&S has been an active participant in the working groups focused on developing these guidelines. We are eager to see the underlying test requirements and associated test assertions that will accompany these guidelines as it is these test requirements and assertions that will

provide the specific information needed to fully guide our efforts to comply with VVSG 2.0. As an example, VVSG 2.0 guideline 9.4 states that “The voting system shall support efficient audits.” ES&S systems currently support audits, and we are actively enhancing these systems to enable even more robust audit support. We are keen to understand the test requirements, assertions, and details related to “efficient audits” so we can ensure our solutions comply with these new standards. We will continue to be active participants in the VVSG 2.0 working groups and look forward to the availability of the test requirements and assertions that will guide our systems development efforts.

3. Do you anticipate producing systems that will be tested for compliance with VVSG 1.1? Why or why not?

The jurisdictions we serve have been requesting systems focused on security improvements and robust support for election audits that are above and beyond the VVSG 1.1. These requests, combined with our recognition that the elections ecosystem must stay ahead of security threats, have resulted in stronger security and auditing advancements. Consequently, ES&S has shifted its focus to compliance with the newer VVSG 2.0 to allow ES&S systems to advance to the higher standards of increased security and auditing.

4. What steps, if any, are you taking to enhance the security of your oldest legacy systems in the field, many of which have not been meaningfully updated (if at all) in over a decade?

ES&S is continually developing new products and conducting research to further security. In fact, the equipment ES&S sells today contains some of the most secure voting technology available.

ES&S takes an active approach to do everything we can with customers who operate legacy systems to help ensure that such systems are as secure as possible, offering regular hardware maintenance and federally-certified software and firmware updates as allowed.

To help deliver accurate election results and maintain the security of legacy systems, we provide support and guidance to election authorities on best practices in conducting pre-election logic and accuracy (L&A) testing, election day operations and post-election audits. We work closely with local jurisdictions to implement physical security controls and proper chain-of-custody procedures for all aspects of the election management and voting systems.

ES&S has conducted “Secure the Vote” seminars around the country to help election administrators ensure their elections are secure, regardless of which systems they are operating. The seminars cover not only the security of the election systems, but also aim to educate election administrators about general best practices in cybersecurity.

Recognizing the challenges that come with a rapidly advancing technology environment, ES&S has worked to architect its current, purpose-built systems to sustain a long useful life, beyond what is expected with typical consumer electronics. As a result, some of our current products have been fielded for well over a decade, yet continue to receive regular security updates and feature enhancements.

5. *How do EAC certification requirements and the certification process affect your ability to create new election systems and to regularly update your election systems?*

The certification process under the EAC Testing and Certification Program varies depending upon the scope and magnitude of the changes to the voting system. A new voting system could potentially take 18 months or more to get through full testing and certification. Modifications to previously certified voting systems generally require 5-7 months, again depending on the scope of changes. Very minor modifications such as a small software revision or a minor hardware modification can potentially complete the EAC process in approximately six weeks.

While the current certification process has served the nation well for over a decade, it is currently in need of modernization. Specifically, the process needs to be streamlined, while maintaining rigor, to better allow for modifications (especially as it relates to COTS) to more quickly address vulnerabilities that may be identified. This is an area where Congress can help.

6. *Do you support federal efforts to require the use of hand-marked paper ballots for most voters in federal elections? Why or why not?*

ES&S fully supports the use of paper ballots for all elections.

ES&S provides both hand-marked and machine-marked (ballot marking device) paper-based tabulation systems. Jurisdictions decide which system and configuration best fit their needs. All paper-based voting machines currently sold by ES&S allow the voter to review and verify their ballot information in the form of human-readable text that is presented to them on a piece of paper.

Using only hand-marked paper ballots is a concern for the disability community as it would separate and segregate certain voters, prohibiting them from participating in a fully universal voting experience. Fully ADA-compliant, ballot marking devices offer the same experience for all voters, regardless of ability, while also utilizing a variety of functions to ensure election data and cast vote records are secure. Ballot marking devices allow voters to review their selections and verify that their vote selections were recorded accurately before submitting for tabulation. Ballot marking devices also eliminate the need for human interpretation of voters' intent when ballots contain marginal or ambiguous marks. To be clear, election systems that process hand-marked paper ballots and election systems that process machine-marked paper ballots are both very secure. We actively sell and support both types of systems, and we do not believe that the federal government should mandate one of those systems over the other. That choice should be left to individual jurisdictions.

7. *How are you working to ensure that your voting systems are compatible with the EAC's ballot design guidelines (i.e. "Effective Designs for the Administration of Federal Elections")?*

ES&S has fully embraced the EAC's ballot design guidelines and uses these as standards within its products. ES&S was intimately involved in the project that led to the development of the best practices prescribed in "Effective Designs for the Administration of Federal Elections." ES&S took part in early pilots, implementing and testing the ballot-design best practices in three counties. This opportunity allowed ES&S to understand the best practices better and adapt our products to enable usage of them. While the final layout and design of ballots is ultimately decided by our customers, we continue to

conduct usability testing and consult with design experts to ensure our products are both highly usable and accessible.

8. *Experts have raised significant concerns about the risks of ballot marking machines that store voter choice information in non-transparent forms that cannot be reviewed by voters (i.e., such as barcodes or QR codes), noting that errors in the printed vote record could potentially evade detection by voters. Do you currently sell any machines whose paper records do not permit voters to review the same information that the voting system uses for tabulation? If so, do you believe this practice is secure enough to be used in the 2020 election cycle?*

Both hand-marked paper ballots and machine-marked paper ballots are highly secure methods of casting a vote. Post-election audits can fortify the security of the election under either voting scenario.

There are several important facts about how tabulators count hand-marked paper ballots and machine-marked paper ballots.

Barcodes exist on both hand-marked paper ballots and machine-marked paper ballots and those barcodes are used in the very same manner in both scenarios to count votes. Here is how tabulation devices read hand-marked paper ballots:

- On a hand-marked paper ballot there is a master barcode along the left edge of the ballot and the top and/or bottom of the ballot.
- When a voter hand marks the oval next to candidate Jane Doe, for example, and inserts that hand-marked paper ballot into a tabulation machine, that tabulation machine is not reading the name Jane Doe. In fact, the tabulation machine does not recognize the text, Jane Doe, at all. Rather, the tabulation machine first recognizes, through digital imaging technology, that an oval has been filled in. Then it uses the master barcode on the ballot to determine the grid coordinates of that filled-in oval.
- In this example, if the grid coordinates of the filled-in oval are “six down, four across,” the tabulation machine then queries the database that resides on the master media (typically a USB stick) that has been inserted into the tabulator. In essence, the tabulation machine asks the database on the master media, “what candidate’s name is associated with six down, four across?” The database, which has been pre-programmed and tested by the county/city election office, then tells the tabulation machine that “six down, four across” corresponds with Jane Doe. At that point, the tabulation machine creates a cast vote record that records a vote for the name Jane Doe.

Jurisdictions perform pre-election logic and accuracy tests and post-election audits to ensure the accuracy of the aforementioned process. During both the pre-election tests and the post-election audits, jurisdictions are asking whether the actual text next to the filled in oval on the hand-marked paper ballot corresponds exactly to the vote that was registered by the tabulation machine. This verification can only be done if the jurisdiction has access to the paper ballot *and* the cast vote record from the tabulation machine. As noted above, pre-election testing and post-election auditing provide a testable and auditable method to verify that ballots are programmed and counted as intended.

Machine-marked paper ballots behave in the exact same way, only the voter marks their ballot with a machine instead of a pen. Here's how:

- When the voter chooses Jane Doe on the touch screen, the marking device prints out a paper record that shows the text Jane Doe along with a barcode that contains the ballot coordinates of "six down, four across." When that paper record is inserted into the tabulator, it performs the same routine as it does with the hand-marked paper ballot. It reads the barcode, which reveals the grid coordinates of "six down, four across" and then it queries the database on the tabulation machine (which is the same tabulation machine that counts the hand-marked paper ballot) asking which candidate name is associated with those grid coordinates. The database then reveals to the tabulation machine that "six down, four across" corresponds to Jane Doe. At that point, the tabulation machine creates a cast vote record for Jane Doe.

Just as is the case with hand-marked paper ballots, the tabulation machine is only looking for the grid coordinates, and the cast vote records from both examples are identical.

Even tabulation systems that utilize Optical Character Recognition (OCR) incorporate the use of a barcode to count the vote. Here's why: It is possible that there could be two separate and distinct candidates, both named Jane Doe, who are running for different offices on the same ballot. The system cannot use OCR to read "Jane Doe" and record a vote reliably because it would have to know for what race the vote for "Jane Doe" should be counted. Thus, the barcode is used to tell the tabulation machine for what race Jane Doe should receive a vote.

In sum, all tabulation machines that count paper ballots use a barcode to determine how to properly and accurately count the vote. The security of each method of voting is confirmed by election officials during pre-election tests and in post-election audits.

9. Do you make voting systems with Cast Vote Records (CVRs) that can be reliably connected to specific unique ballots, while also maintaining voter privacy? If not, why not? Does your company make voting systems that allow for a machine-readable data export of these CVRs in a format that is presentation-agnostic (such as JSON) and can be reliably parsed without substantial technical effort? If not, why not?

ES&S high-speed central scanners can imprint a ballot identification number on a ballot. This ballot identification number allows the paper ballot to be directly tied to a cast vote record while maintaining strict voter privacy. This capability is currently being added to our precinct scanner.

ES&S solutions do provide a cast vote record export in a flexible format. The imprinted ballots and the cast vote record exports have been used in multiple jurisdictions, most recently in the State of Rhode Island, to successfully complete post-election risk-limiting audits.

10. Would you support federal legislation requiring expanded use of routine post-election audits, such as risk-limiting audits, in federal elections? Why or why not?

Yes, ES&S strongly supports legislation that would expand the use of routine post-election audits.

ES&S believes that successful post-election audits, including risk-limiting audits such as those which have recently occurred in several jurisdictions, will increase confidence in our country's election process.

11. What portion of your revenue is invested into research and development to produce better and more cost-effective voting equipment?

Over the last four years, our research and development expenses have averaged approximately 19 percent of our revenue.

12. Congress is currently working on legislation to establish information sharing procedures for vendors regarding security threats. How does your company currently define a reportable cyber-incident and what protocols are in place to report incidents to government officials?

ES&S follows the 2018 Department of Homeland Security publication, "Incident Handling Overview for Election Officials," which instructs election entities how to inform DHS about cyber-related incidents. Also, ES&S has a mature, tested incident-response policy and process whereby potential cyber incidents are triaged by our internal team of subject matter experts. Where circumstances indicate the reporting of the incident to government officials, we follow DHS guidelines for alerting the National Cybersecurity and Communications Integration Center (NCCIC), Multi-State Information Sharing and Analysis Center (MS-ISAC), and EI-ISAC.

ES&S hosted a tabletop exercise at our headquarters just prior to the November 2018 General Election that was facilitated by the DHS National Cyber Exercise and Planning Program (NCEPP) team from the NCCIC. During this exercise, we reviewed and practiced our established protocols for analyzing and reporting incidents to the proper government officials.

13. What steps are you taking to improve supply chain security? To the extent your machines operate using custom, non-commodity hardware, what measures are you taking to ensure that the supply chains for your custom hardware components are monitored and secure?

Our purpose-built tabulation machines, which are produced in ISO-9001 manufacturing facilities, are made of many commercially available components configured to a custom design for a specific use. The entire voting system is managed by a secure engineering change order control process. This includes all component suppliers. Changes to the voting system follow a formal closed-loop process and must be internally and externally reviewed, verified, tested and approved before they can be incorporated into the voting system. Every unit is individually serialized for complete traceability.

ES&S also conducts thorough security reviews of our supply chain including supply-chain risk assessments and on-site visits to our suppliers to ensure that every component is trusted, tested and free of malware. All tabulation software is developed and compiled exclusively in the USA. All components of the hardware go through a formal incoming inspection and testing process. Final hardware configuration control and quality assurance are performed at our headquarters in Omaha, Nebraska.

As standard practice, each hardware and software release undergoes thousands of hours of performance testing and runs millions of test ballots along with extensive security testing after which ES&S provides a complete set of software components to the voting systems testing labs (VSTL) for review.

In addition, ES&S is participating in discussions with the Department of Homeland Security's National Risk Management Center (NRMCC), the National Institute of Technology (NIST) and the Center for Internet Security (CIS) regarding the development of guidelines and best practices to ensure that we continue to manage new or emerging risks associated with supply chain components.

14. Do you employ a full-time cybersecurity expert whose role is fully dedicated to improving the security of your systems? If so, how long have they been on staff, and what title and authority do they have within your company? Do you conduct background checks on potential employees who would be involved in building and servicing election systems?

Yes, Mr. Chris Wlaschin is ES&S' Vice President of Systems Security and Chief Information Security Officer. Mr. Wlaschin reports directly to me. He has worked for ES&S for a year, and he has the authority to drive security improvements across hardware, software, and corporate operational and infrastructure security. Mr. Wlaschin is also the Chair of the Elections Infrastructure Subsector Coordinating Council (EI-SCC), a DHS sponsored organization to drive security improvements across the elections industry. Prior to joining ES&S, Mr. Wlaschin was the Chief Information Security Officer for the Department of Health and Human Services in Washington D.C., where he oversaw cybersecurity efforts for the Department. He has held other senior cybersecurity leadership positions in both the public and private sector including the Department of Defense, Department of Veterans Affairs, National Research Corporation, and the University of Nebraska.

ES&S conducts thorough background checks on all employees and we contractually require our vendor partners to do the same. Every employee at ES&S is expected to be accountable for security and all receive annual security training; it's an essential part of everyone's job.

15. Does your company operate, or plan to operate, a vulnerability disclosure program that authorizes good-faith security research and testing of your systems, and provides a clear reporting mechanism when vulnerabilities are discovered? If not, what makes it difficult for your company to do so, and how can Congress and the federal government help make it less difficult?

ES&S is actively working with good-faith ethical researchers to test our systems. We also provide a security message and email address on our public website that states "If you have a comment about election security or would like to report an issue, potential vulnerability or bug to us, please contact us by using the following email address: security@essvote.com. Your comments will be kept confidential, and a member of our security team will follow up with you."

ES&S utilizes its internal corporate information security staff to receive, evaluate and act upon, as necessary, unsolicited vulnerability reports from cybersecurity researchers and other third parties. These unsolicited reports may be received by phone, verbal, mail or media reports.

Congress and the federal government can help the election sector by proposing legislation to create and support an Independent Coordinated Vulnerability Testing and Disclosure Process to improve election system security across all election vendors. This cybersecurity testing program would mandate that all voting machine vendors submit their systems to a programmatic cyber testing program conducted by vetted and approved researchers. Although voting machines are not connected to the internet, there are non-internet related types of cybersecurity testing that are necessary to protect elections. Machine penetration tests simulate attacks on election equipment by people who gain physical access to the voting machines or the components.

Congress could also pass legislation that requires a paper record for every voter. It is difficult to perform a meaningful audit without a paper record of each voter's selections. Mandating the use of a physical paper record sets the stage for all jurisdictions to perform statistically valid post-election audits.

ES&S believes if Congress can establish these standards, the general public's faith in the process of casting a ballot can be restored.

16. How will DARPA's work impact how your company develops and manufactures voting machines?

We are very interested in learning more about the DARPA effort and how we can potentially leverage the work that emerges from the DARPA effort into ES&S products to improve election security. We have established contact with individuals involved and are seeking to find ways to participate, learn, and contribute.

We know that improving the confidence of every voter requires a tight collaboration between federal, state and local election officials, the EAC, DHS, law enforcement, voting system manufacturers, and the election community at large. As an American company and the nation's leading election provider, ES&S is committed to delivering high security products and services to ensure the integrity of our nation's elections.

Thank you for allowing ES&S to share our approach and all of the proactive steps we and our customers have taken and continue to take to secure the cornerstone of our democracy.

Yours truly,



Tom Burt, President & CEO
Election Systems & Software



November 18, 2020

Certification

Park IP Translations

TRANSLATOR'S DECLARATION:

I, Jerel Pulicicchio, am fluent in both the Portuguese and English languages. I have translated the article titled "Nadaf (original)" from Portuguese to English. I hereby certify that the translation is accurate and complete to the best of my judgment and ability. I understand that willful false statements and the like are punishable by fine or imprisonment, or both, pursuant to 18 U.S.C. § 1001.

I certify under penalty of perjury under the laws of the United States that the foregoing is true and correct.

Jerel Pulicicchio

Jerel Pulicicchio

Project Number: BBLP_2010_P0432

15 W. 37th Street 8th Floor
New York, NY 10018
212.581.8870
ParkIP.com

Ex. 2007 / PGR2025-00066 / Page 68 of 557

Election Systems & Software, LLC v. Hart Intercivic, Inc., PGR2020-00031, Page 1

[coat of arms of Brazil]

Federative Republic of Brazil
Ministry of Development, Industry and
Foreign Trade
National Institute of Industrial Property

(22) Filing Date: 07/19/2013 (43)
Publication Date: 09/02/2014 (RPI
2278)

[barcode]
* BR 10 2013 018558 A 2 *

(51) Int.Cl.:
G07C 13/00
G06K 9/46
G06Q 50/00

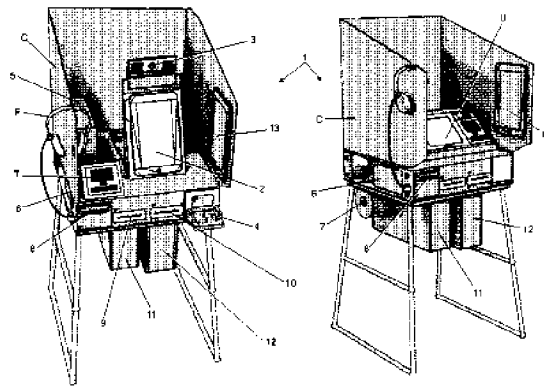
(54) Title: SECURE VOTER BALLOT PRINTING AND COLLECTION EQUIPMENT AND EQUIPMENT FOR AUDITING AND COUNTING OF VOTES PRINTED ON SECURE BALLOTS, FOR THE MECHATRONIC VOTING SYSTEM

(73) Owner(s): Ronaldo Moisés Nadaf

(72) Inventor(s): Ronaldo Moisés Nadaf

(74) Attorney(s) in fact: MODAL MARCAS E PATENTES LTDA

(57) Summary: SECURE VOTER BALLOT printing and collection equipment AND EQUIPMENT FOR AUDITING AND COUNTING OF VOTES PRINTED ON SECURE BALLOTS, FOR THE MECHATRONIC VOTING SYSTEM", where one equipment (1) forms a system that allows the voter to vote and obtain a printed ballot (14) by which the electronic vote and printing will be confirmed, by using bar codes (15), (16), (17) and (18) recorded on it. This ballot (13) is transferred to a second equipment (19), for the counting of the votes, where such information will be read, forming an electronic and printed storage system, in total interaction and subject to being audited, in case of doubts regarding fraud, providing total security to the electoral system.



“SECURE VOTER BALLOT PRINTING AND COLLECTION EQUIPMENT AND
EQUIPMENT FOR AUDITING AND COUNTING OF VOTES PRINTED ON SECURE BALLOTS,
FOR THE MECHATRONIC VOTING SYSTEM”

This invention patent application is in reference to a set of equipment that will ensure the electronic
5 voting of any citizen combined with the possibility of providing a certified record of their political
intention, by using paper voting ballots as a mechanism for auditing and securing individual votes.

This set of equipment will bring the vote printed on paper ballots to the electoral process,
however, with another level of security, where the ballot printed with the citizen's vote on it will only be
handled by the voting voter.

10 The first equipment, entitled SECURE VOTER BALLOT PRINTING AND COLLECTION
EQUIPMENT, will allow, in addition to printing the vote, to increase the security of voter identification,
as its objective is to provide a process with double voter biometric recognition, where, in addition to the
fingerprints of 4 fingers of the hand being verified, a biometric face recognition will also be used as
verification.

15 The voter ballot produced in this new technological context will provide for the printing of at
least 2 individual voting records, with the first text record being produced by the digital systems of the

20

digital voting equipment, including the electronic ballot boxes in use today, and a second registration of the vote, which will be generated by the SECURE VOTER BALLOT PRINTING AND COLLECTION EQUIPMENT, object of this patent, said printed vote, on the same ballot, in two-dimensional barcodes, further expanding the security, transparency and the mechanisms for auditing the process of generating and collecting votes.

In addition to the two individual voting records, one in text and the other in the form of a barcode, the printed ballot will provide two more records in the form of a two-dimensional barcode that will store the digital signatures from the Electoral Judiciary and another institution responsible for auditing the process.

Said digital signatures will be produced by asymmetric cryptography based on the ECDSA (Elliptic Curve Digital Signature Algorithm) algorithm, with a minimum key pair size of 283 bits. The voting signature process will take place using the private keys of the institutions, which will be installed on the SECURE VOTER BALLOT PRINTING AND COLLECTION EQUIPMENT and on the computer collecting the votes, ensuring the validity of the institution of origin printed on the vote, without violating its secrecy.

A second piece of equipment included in this patent application herein, entitled EQUIPMENT FOR AUDITING AND COUNTING OF VOTES PRINTED ON SECURE BALLOTS, will be responsible for controlling the receiving from the ballot box containing the printed ballots, while said ballot box will have its physical security maintained by a seal with

radio frequency technology [RFID].

This equipment, in addition to controlling the radio frequency seals, will audit the printed votes collected in the ballot box, by comparing the text record to the information contained in the two-dimensional barcodes, verifying the digital signatures against the respective public keys generated for the voter ballot collection equipment, confirming the validity of the institution of origin and the integrity of the content of the printed vote.

Only after being audited will the printed vote be validated for the counting of the vote, which will be counted electronically with the other votes of the voting site in a simplified system of vote accounting, also installed in the EQUIPMENT FOR AUDITING AND COUNTING OF VOTES PRINTED ON SECURE BALLOTS.

This machine will also be responsible for the packaging of the printed ballots collected at a voting site, which will come out of this second equipment, totaled and sealed in a plastic wrapper with another chip of radio frequency identification technology, which initiates the process of storage and auditing controlled by this technology.

STATE OF ART

As is known historically, there are cultural traumas caused by the period when the country [Brazil] held its elections by using paper ballots.

Many frauds occurred during this long period from the distant past,

as for example the chain vote (*voto carreirinha*), when a first voter managed to leave with a blank ballot of the voting site, passed it on to a corrupt individual who completed the ballot with the name of his/her candidate and handed it over to another voter who inserted the previously filled out ballot and repeated the operation of withdrawing a blank ballot, thus making a safe, and evidently illegal, cycle for diversion of votes.

Reports of counterfeiting, adulteration and loss of ballots are part of a distant past because they were effectively extinguished with the current electronic voting model. Therefore, the general population and also the political class do not believe in the actual need to print the vote on paper.

However, they are apprehensive about adhering to completely electronic voting. This statement is due to the fact that scientific research developed by several countries, which seeks to improve the security and transparency of their electronic voting processes, increasingly points to the need for voters, especially the lay voter, in terms of technology, to have the possibility to check if their voting intention was recorded and accounted for correctly without risking losses caused by errors, which unfortunately are present in completely electronic voting.

Several studies on electronic voting reveal the need for a physical audit trail of individual voting, where the voter, only with his/her eyes, can be guaranteed that his/her vote will not suffer

any possibility of adulteration or loss and thus, ensuring that it will be included in the total for the final result of the election.

In this context, in the year 2000, in the postdoctoral thesis proposed by Ph.D. Rebecca Mercuri, entitled “Electronic Vote Tabulation - Checks & Balances”, the concept of “Voter-verified Paper Audit Trail (VVPAT)” and “ Verified Paper Record (VPR) “ was put fourth, which, in summary, discusses the importance of the existence of a paper audit that will allow for the recount of the votes of an electronic election, when necessary.

In 2006, Ronald Rivest who has a Ph.D. in cryptology , along with a researcher from the National Institute of Standards and Technology in the United States, John Wack, idealized the concept of “software independence” for electronic voting processes. These scientists argue that “a voting system is software independent if an (undetected) change or error in its software cannot cause an undetectable change or error in an election outcome.”

Also noteworthy is the technical standard that is being improved by the Institute of Standards and Technology (NIST) and by the Electoral Assistance Commission of the United States of America, known as the “Voluntary Voting System Guidelines” that brings fourth in the draft of the most current version, the following minimum requirements for approval of voting equipment in that

country (back-translated from Portuguese):

a - At least two records of voter selections are produced and one of the records is then stored such that it cannot be modified by the voting system, so that both records are not under the control of a single digital process;

5 b) - The voter must be able to verify that both cast vote records are correct and match before leaving the polling place;

c) The verification processes for the two cast vote records must be independent of each other, and at least one of the records must be verified directly by the voter;

d) The contents of the two cast vote records also can be checked later for consistency
10 through the use of unique identifiers that allow the records to be linked.

In Brazil, article 5 of Law No. 12,034/94 is emphasized, which amends the Political Parties Law (9,096/95), the Elections Law (9,504 / 97) and the Electoral Code (4,737/65), which requires the use of vote printing devices since the 2014 elections.

The article is suspended by a preliminary decision issued in the Direct Action of
15 Unconstitutionality No. 4547 filed with the Federal Supreme Court by the Office of the Attorney General of Brazil. The lawsuit questions the printed vote described in the law, which, in theory, violates the voter's right to secrecy.

In view of this scenario, it can be seen that the Brazilian electronic ballot box was no longer compliant with the applicable laws, nor did it meet the basic requirements

20

of the North American standard, for being a DRE (Direct-Recording Electronic) collector and counting system, characterized by direct electronic recording without printing the vote for the voter's verification.

PURPOSE OF THE PATENT:

The purpose of the equipment, which is the object of this invention patent application herein, is precisely to increase the security of the electoral process as a whole and was designed in a manner, in which the ballots printed on the devices will be handled exclusively and only by the voter himself/herself thus reducing the range of possibilities for electoral fraud that occurred mainly in the act of counting paper ballots.

For this purpose, the proposed model is composed of a secure ballot, with the vote in text format and a second record of the vote in the form of a two-dimensional barcode, which uses an information encoding bar graph technology for which the license to use is free of royalties.

The vote in the text format produced for the ballot will be generated in an electronic vote recording device (Direct Recording Electronic - DRE), which may even be the electronic ballot box in use today, which will be connected, via USB port, to the SECURE VOTER BALLOT PRINTING AND COLLECTION EQUIPMENT.

Through the system, the user will be able to vote electronically, which, once completed, will generate the printed vote, providing certainty to him/her of his/her choice and preventing equipment failures from

20

losing the vote cast digitally.

To explain superficially, they pass through the two pieces of equipment and the systems that surround them, which will be better detailed in the attached drawings, through which it can be seen:

Figure 1 - shows, on the left, the SECURE VOTER BALLOT PRINTING AND COLLECTION
 5 EQUIPMENT connected to a Tablet and, on the right, the same equipment connected to the Electronic Ballot Box;

Figure 2 - shows the SECURE VOTER BALLOT PRINTING AND COLLECTION EQUIPMENT and, on its side, enlarged details of the biometric readers;

Figure 3 - shows, in enlarged detail, the interfaces of the SECURE VOTER BALLOT PRINTING
 10 AND COLLECTION EQUIPMENT;

Figure 4 - shows the secure ballot of the vote, with its digital codes;

Figure 5 - shows the independent ballot box being connected to the EQUIPMENT FOR AUDITING AND COUNTING OF VOTES PRINTED ON SECURE BALLOTS;

Figure 6 - shows the EQUIPMENT FOR AUDITING AND COUNTING OF VOTES
 15 PRINTED ON SECURE BALLOTS;

Figure 7 - shows the EQUIPMENT FOR AUDITING AND COUNTING OF VOTES PRINTED ON SECURE BALLOTS. The packaging devices are highlighted in the details;

20

Figure 8 - shows the sealed ballots, forming a stack controlled by RFID technology.

In accordance with the attached drawings, the “SECURE VOTER BALLOT PRINTING AND COLLECTION EQUIPMENT”, one of the pieces of equipment subject to this invention patent application, consists of one piece of equipment (1) enclosed by a voting booth (C) that can be connected
 5 to an electronic ballot box (U), as shown in figure 1, said equipment (1) in the form of a computer with a reversible keyboard and touch screen or a tablet (2), with headphones (F), connected to a camera (3) with capacity to perform biometric recognition of the voter's face and connected to a mechanical keyboard (T) reused in the process of recycling the ballot boxes.

The equipment (1) has a bench on which a four-finger biometric reader is installed (4), blank
 10 ballot storage (5) connected to its printer (6), also fed by a spool of paper (7), both communicating with one printer output device (8). The bench also has an input device (9) that verifies and collects the printed ballots confirmed by the voter, in addition to an input device (10) that verifies and shreds a printed ballot that was rejected (canceled) by the voter.

The input device that verifies the printed ballots confirmed by the voter (9) is connected to an
 15 independent collector (11) of ballots confirmed and verified by the system, whereas the input device

that verifies and shreds a printed ballot that was rejected by the voter (10) is connected to an ecological ballot box (12) that receives the shredded pieces from these printed ballots that were rejected by the voters, thus forming the equipment (1) itself, as shown in figures 1, 2 and 3.

The equipment (1) that prints and collects the secure voter ballots [SECURE VOTER BALLOT
5 PRINTING AND COLLECTION EQUIPMENT] is completed by a second tablet (13), where software developed by an electoral process auditing entity will be installed, containing the public keys of the respective units of equipment. This equipment (13) will be used by the voter to electronically verify the vote printed in the two-dimensional bar code, allowing him/her to leave the polling station after checking the two printed records of his/her vote, one in text and the other in the form of a two-dimensional barcode.

10 Assembled in this manner, the equipment (1), integrated with open source software to be developed, will be used as a voting booth for a novel system for collecting electronic votes and votes printed on paper, with double biometric identification activated by the voter himself/herself.

The voter places the four fingers of his/her right hand on the biometric identification reader (4), when the equipment (1) then collects the biometric data and sends a digitally signed request to the
15 electronic voting system installed on the computer or tablet (2).

In front of the equipment (1), the voter is also identified by the camera (3) that will perform the biometric face recognition.

Once the voter's double biometric identification is completed, he/she will have

20

access to the voting interface or, in the case of an illiterate voter, as previously identified, direct access to the interface specifically developed for uneducated voters.

By pressing the corresponding key on the screen (2), or through the reused mechanical keyboard of the Electronic Ballot Box (T), the voter chooses his/her candidates, which shows the respective photographs and other possible information. The candidate's photograph is displayed on the said screen
5 (2) so that the voter may recognize his/her choice and confirm the digital vote.

After the electronic vote has been collected, the voter authorizes, on the screen (2) or on the mechanical keyboard (T), the printing of one secure ballot (14) that will be emitted by the printer output device (8).

10 The secure ballot (14) for the vote, shown in figure 4, will show the voter's choices for each elected position being disputed in that election and / or referendum, explicit in sufficiently legible text. The ballot (14) will also show the complete vote of the voter encoded in the form of a two-dimensional barcode, which will also contain digital signatures from the Electoral Judiciary and another institution auditing the process (15).

15 Two more barcodes (16) and (17), of smaller size and reduced storage capacity, will be printed on the ballot (14) and will each bear a digital signature, now referring to the vote text printed on the ballot (14), produced by the Electoral Judiciary and another entity auditing the process, respectively. The ballot (14) will also have an electronic code in Braille (18) for visually impaired voters.

20

With the printed secure ballot (14) in hand, the voter will also be able to check the bar-coded vote on the second tablet (13), which will read the code and display the record of the coded vote on the screen.

After confirming that the text and record of the code are each translating their political intention, the voter inserts the ballot (14) into the vote confirmation input device (9).

5 The equipment (1) then electronically reads, the barcode(s) (16) or (17) and (18) on this ballot (14), extracting the institutional digital signatures.

Once confirmed that that signature was generated by the private key issued for the institutional digital signature, that is, after confirming the electronic origin of the ballot (14), it is sucked into the mechanical device of the vote confirmation input device (9) and stored in a randomized order in the
10 independent ballot box collector (11). This signature check will prevent the equipment from being fed by ballots not officially produced.

After the voting collection operation is completed, the equipment (1) sends a digital signal to the electoral system to record the digital registration of the vote and terminate the possibility of a new vote being cast for that voter. In this manner, the vote is counted in the standard manner.

15 If the voter does not agree with the vote on the printed ballot (14), desisting or realizing that he/she made a mistake, while intending to correct said vote,

20

the voter will insert the said ballot (14) into the verifier and shredder input device (10) for rejected printed votes and, once the equipment (1) confirms the signature produced by the institutions' private key and the origin of the ballot (14) is confirmed, it is then sucked in and shredded and the paper waste will be stored in the ecological ballot box (12), sending a signal to the electoral system installed on the computer of equipment (1) to cancel the digital vote and restart the voter identification process, which restarts the entire voting process to the initial stage.

This makes it possible for the vote printed by the voter himself/herself to be corrected. In this case, the rejected vote is not counted in the system's database, which prevents erroneous counting at the end of the voting and allowing the voter to have another chance or option to vote, without contaminating the entire process with ballots rejected by voters.

If the voter is illiterate, the vote can be cast using the fliers previously distributed by the candidates with the two-dimensional barcode on them.

Following the double biometric identification, the illiterate voter in possession of this advertising material printed by the candidates with a two-dimensional bar code, will insert the flier in the verifier shredder input device (10), and upon viewing the photo of their candidate on the screen (2), the operation is then repeated until the end of the process, when the secure ballot (14) will be printed, to be confirmed immediately by the uneducated voter, who

20

should be instructed to insert the ballot (14) with the vote into the vote confirmation input device (9).

The same flier reading procedure can be used to assist the vote of visually impaired voters, however, instead of confirming the vote shown on the screen (2), the visually impaired voter will confirm his/her digital vote by using a headset (F), which will inform the equipment handling instructions (1) for confirming the vote, instructing the disabled voter throughout the complete digital voting process and the destination of the printed vote, which will also be transcribed in the Braille code (18), on the interface of the collector verifier (9). The visually impaired voter may also enter the vote by using the mechanical keyboard (T), which is connected to the equipment (1).

In all scenarios in which the printed vote is confirmed, the voter may print, at the end of the process, a proof of attendance, from the paper spool (7) installed on the lower part of the equipment (1), which will be emitted by the output (8) of the printer.

As noted, the proposed system eliminates the roll of the poll worker.

After the voting is closed, the independent ballot box (11) of confirmed ballots, that is, of confirmed votes, is then removed from the voting equipment (1) and taken to the audit, vote counting and vote totaling area, as shown in figure 5.

In this other area, the independent ballot box (11)

20

of confirmed votes is connected, as shown in figure 5, to the EQUIPMENT FOR AUDITING AND COUNTING OF VOTES PRINTED ON SECURE BALLOTS (19), when the process of auditing and accounting of the votes begins.

This equipment (19), also object of the patent herein, as shown in particular by figures 6 and 7
 5 and also by figure 5, on one of its sides is composed of an input device (20) of an independent ballot box (11) , with a RFID reading/writing device (21) and an audited ballot input device (22). On the other side it has a printer (23) and LCD monitor (24), reused from the Electronic Ballot Box.

On the inside, the equipment (19) has an optical OCR and QR code reader and a CPU (25), along with packing devices (26), communicating, on the other side, with a packaged ballot output device (27)
 10 that will receive a RFID identification to be applied by the labeler (28).

The equipment (19) will be fed by the information provided by the independent ballot box storage (11), or by the sealed secure ballots printed (14), in an audit process, with different functions being performed in a single mechanically automated routine.

If the seal of the independent ballot box (11) confirming the vote has evidence being violated, the
 15 equipment (19) issues an audible and text warning on the LCD screen, with the said independent ballot box (11) being sent to the counting commission, which will decide on whether or not to proceed with the respective counting.

20

The first function of the EQUIPMENT FOR AUDITING AND COUNTING OF VOTES PRINTED ON SECURE BALLOTS (19) is to receive the independent ballot box (11) through the input device (20) and to verify the origin of the seal of the independent ballot box (11) through the radio frequency device (21) and, once the relationship between the chip and the voting site is confirmed, the
 5 printed votes are automatically withdrawn from the said independent ballot box (11).

The ballots (14) then pass through the optical reader (25), which will read the barcodes (16), (17) or (18), extracting and verifying the digital signatures, while also comparing the voting information in text to the vote information encoded in the barcode.

After a comparative audit, the printed vote is then counted electronically and sent to a module
 10 (26) where, together with the other ballots (14) of the voting site being counted, they will be stored. Once the total counting of the votes is completed, the ballots will be sealed in plastic and sent out (27), forming a stack of paper (29), as shown in figure 8, which will receive a radio frequency chip in the labeling machine (28), thus concluding the process of auditing and electronic counting of the printed ballots.

The votes included in the audit (22), will receive the ballots that required an additional inspection
 15 process. The procedure for counting audited ballots is similar to the procedure of the ballots collected, differing only in the origin of the information of the radio frequency

identification, that is, instead of reading the RFID seal of the independent ballot box, the interface will read an RFID identifier from a stack of ballots where the need for a more refined audit was detected.

For security purposes, the EQUIPMENT FOR AUDITING AND COUNTING OF VOTES PRINTED ON SECURE BALLOTS (19) is devoid of an input device, which only has the storage disk for the mechatronic device control programs and that of interpretation, auditing and accounting of the printed votes.

Reports, alerts and the final totals bulletin will all be emitted in text format and in the form of a two-dimensional barcode through the printer and recorded in the log file of the machine.

The objective is for this second piece of equipment of the patent herein to be manufactured using electronic components such as processors, memory, printer, LCD screen and plastic components reused from the process of recycling the current electronic ballot boxes, which will be replaced by computers or tablets as they mature throughout the implementation process of the new electronic and mechanical voting equipment that comprise the object of this patent.

CLAIMS

1) "SECURE VOTER BALLOT PRINTING AND COLLECTION EQUIPMENT", with one piece of equipment (1) enclosed by a voting booth (C) that can be connected to an electronic ballot box (U), characterized by a computer configuration with reversible keyboard with a touch screen or tablet (2), headset (F), camera (3) with

5 biometric recognition of the voter's face and connected to a mechanical keyboard (T), with said equipment (1) also being equipped with a bench with a four-finger biometric reader (4), blank ballot storage (5) connected to the printer (6) fed by a paper roll (7), both communicating with a printer output device (8) , with said bench also having an input device (9) that verifies and collects the printed ballots confirmed by the voter, in addition to an input device (10) that verifies and shreds a printed ballot that was rejected

10 (canceled) by the voter, with said input device (9) being connected to an independent ballot box (11) that collects ballots confirmed and verified by the system, and the input device (10) connected to an ecological ballot box (12) that receives the shredded printed ballots that were rejected by the voters, with the said equipment (1) being completed by a second "tablet" (13), installed with software developed by an entity auditing the electoral process, containing the public keys for the equipment, for electronic verification (by

15 the voter himself/herself), of the vote printed in the form of a two-dimensional bar code.

2) "SECURE VOTER BALLOT PRINTING AND COLLECTION

EQUIPMENT”, in accordance with claim 1, the equipment (1), for use with a voting booth, forms a system **characterized** by the collecting of electronic votes and votes printed on paper, with double biometric identification activated by the voter himself/herself.

3) “SECURE VOTER BALLOT PRINTING AND COLLECTION EQUIPMENT”, in accordance
 5 with claim 2, **characterized** by, once the keyboard is used by the voter, a printed ballot (14) will be produced
 (3) with a complete vote encoded in the form of a two-dimensional barcode, with digital signatures from the Electoral Judiciary and another institution auditing the process (15), in addition to barcodes (16) and (17),
 of smaller in size and with reduced storage capacity, along with an electronic code in Braille (18).

4) “SECURE VOTER BALLOT PRINTING AND COLLECTION EQUIPMENT”, in accordance
 10 with claim 2, an electronic cross-checking procedure is performed by the equipment (1) and also by the
 second tablet (13), **characterized** by the ballot (14) being inserted in the vote confirmation input device
 (9) and stored randomly in an independent ballot box (11), with a digital signal being sent for recording
 of the digital voting record by the electoral system.

5) “SECURE VOTER BALLOT PRINTING AND COLLECTION EQUIPMENT”, according to
 15 claim 2, in the event of the vote being corrected, **characterized** by the ballot (14) being inserted in the
 input device (10) for shredding and the digital signal being sent to the electoral system, for the

cancellation of the vote, without being counted, with the voting process being restarted.

6) “SECURE VOTER BALLOT PRINTING AND COLLECTION EQUIPMENT”, in accordance with claim 2, in the case of an illiterate reader, characterized by the use of a flier with two-dimensional bar codes with double biometric identification, followed by the insertion in input device (10) of the shredder verifier, then viewing the candidate's photo on the screen (2), then repeating the procedure until the end of the process, for the printing of the ballot (14) and confirmation by the vote confirmation input device (9).

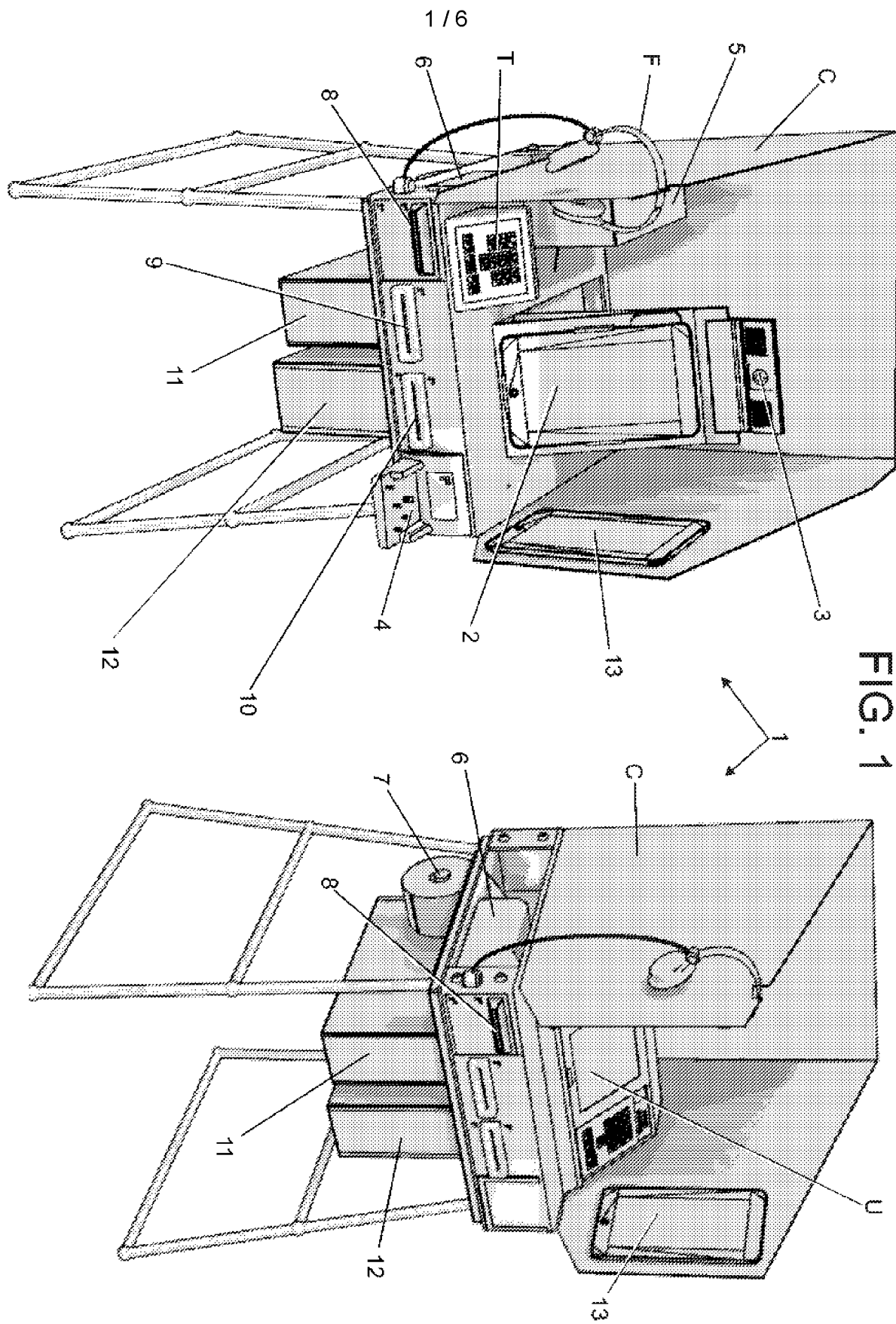
7) “SECURE VOTER BALLOT PRINTING AND COLLECTION EQUIPMENT”, in accordance with claim 2, in the case of visually impaired voters, characterized by casting the vote by using fliers with barcodes or using the mechanical keyboard (T), and confirmation of the vote by using the headset (F), inserting the ballot (14) with the vote transcribed in the form of a Braille code (18) into collection input device (9) or in the shredder input device (10).

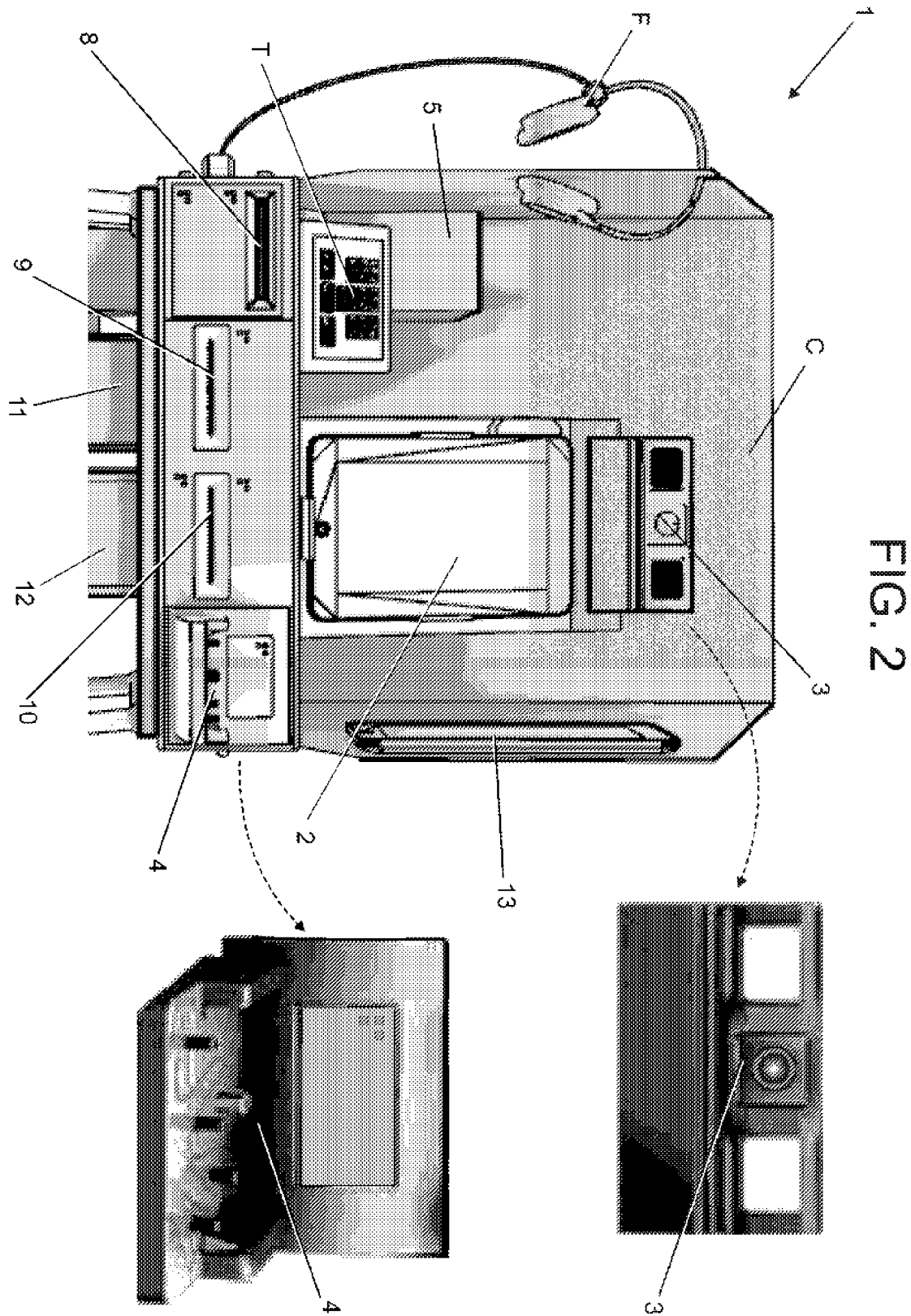
8) “SECURE VOTER BALLOT PRINTING AND COLLECTION EQUIPMENT” accordance with claim 2, after emitting the proof of the vote through the printer's output device (8), characterized by an independent ballot box (11) with the ballots (14) stored, to be removed and inserted in the input device (20) of the EQUIPMENT FOR AUDITING AND COUNTING OF VOTES PRINTED ON SECURE

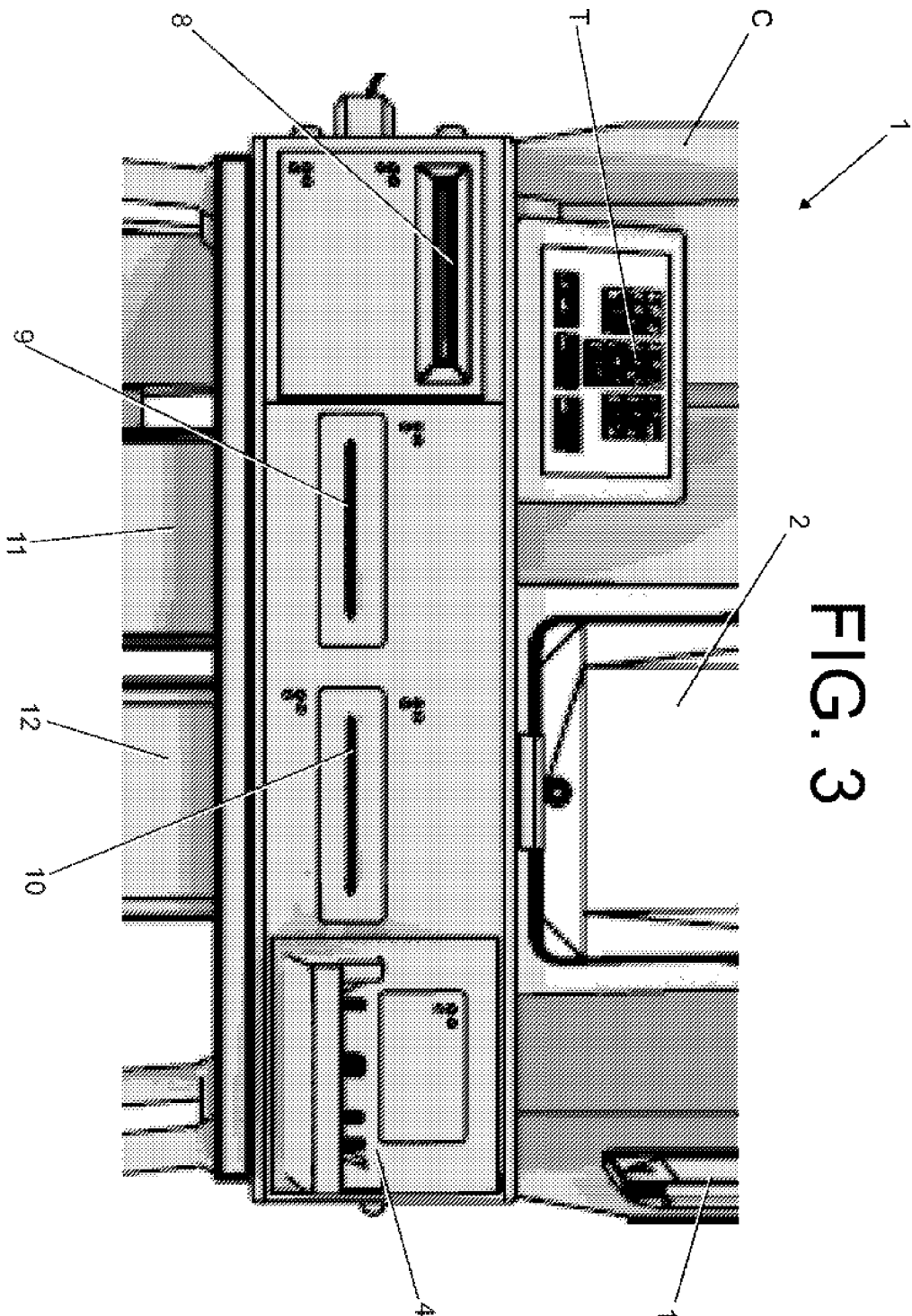
20

BALLOTS also equipped with a RFID reader / writer (21), audited ballot input device (22) with, on the other side, a printer (23) and LCD monitor (24) and, on the inside, an OCR and QR code optical reader and a CPU (25) and packaging devices (26), communicating on the other side, with an output device (27) of packaged ballots, capable of receiving RFID identification by a labeler (28).

- 5 9) “EQUIPMENT FOR AUDITING AND COUNTING OF VOTES PRINTED ON SECURE BALLOTS”, in accordance with claims 2 and 8, form a system **characterized** by reading the information introduced in the independent ballot box (11) with the use of the radio frequency device (21) and, if there are signs of violation, an audible and text warning will be issued on the LCD screen, for electoral reevaluations.
- 10 10) “EQUIPMENT FOR AUDITING AND COUNTING OF VOTES PRINTED ON SECURE BALLOTS”, in accordance with claim 9, **characterized** by the reading of the barcodes (16), (17) or (18), and the electronic counting of the ballots (14), stored in the module (26), followed by the seal, forming a stack (29) emitted from the output device (27), while receiving, in the labeling machine (28), a radio frequency chip, for use with a voting booth, to form a system **characterized** by the collection of electronic
- 15 votes and votes printed on paper, with double biometric identification, activated by the voter himself/herself.







FGW

FIG. 4

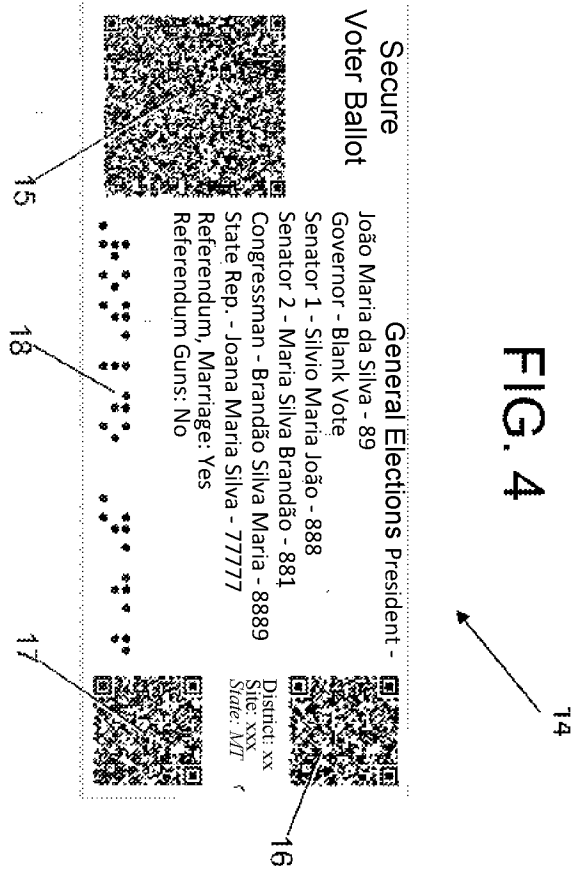
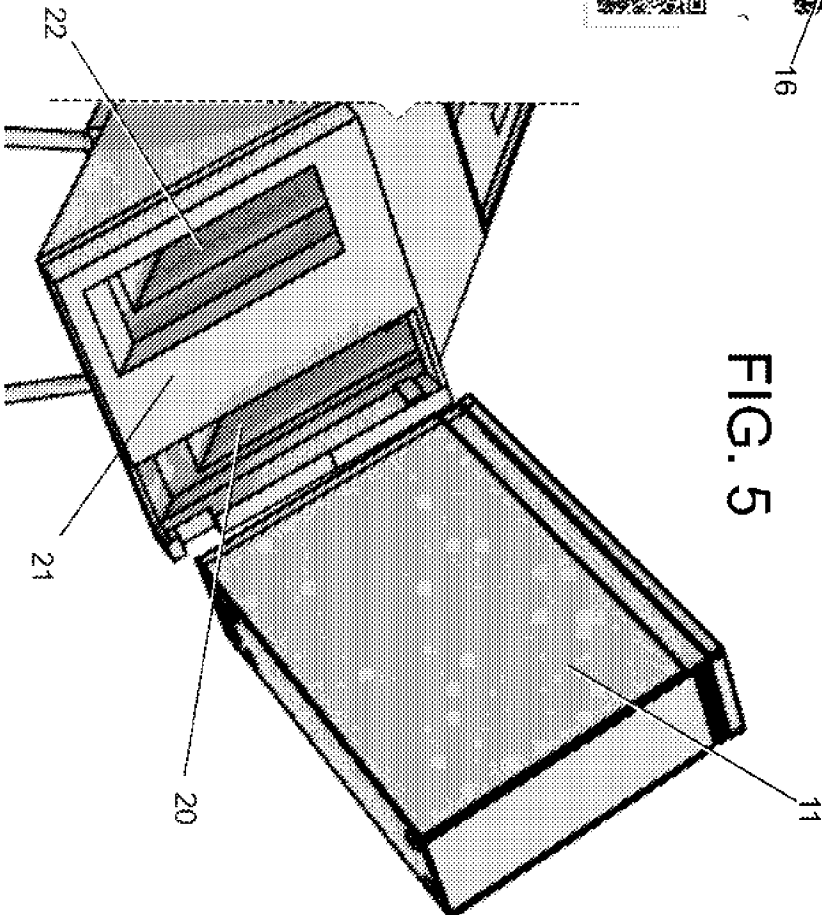
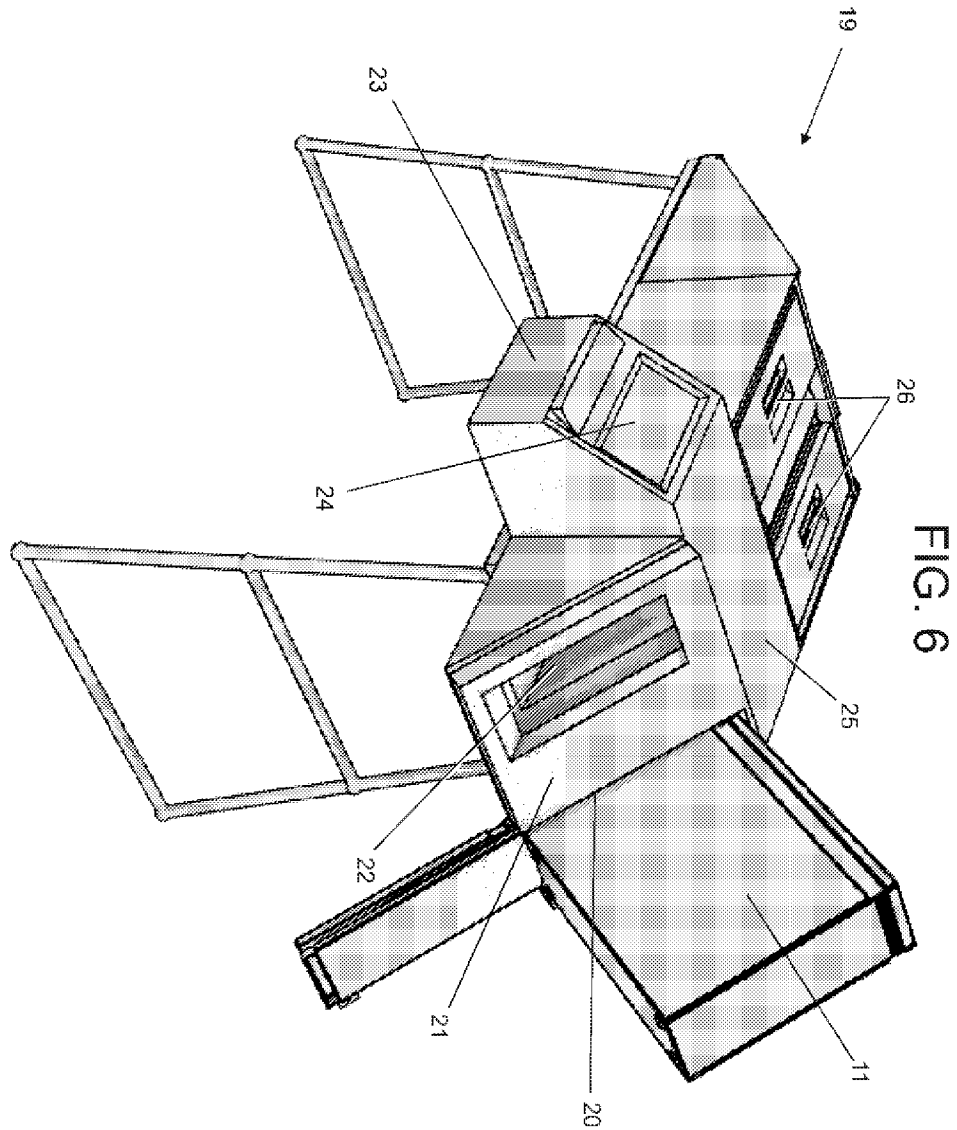


FIG. 5







ABSTRACT

“SECURE VOTER BALLOT PRINTING AND COLLECTION EQUIPMENT AND EQUIPMENT FOR AUDITING AND COUNTING OF VOTES PRINTED ON SECURE BALLOTS, FOR THE MECHATRONIC VOTING SYSTEM”, where one equipment (1) forms a system that allows the voter to vote and obtain a printed ballot (14) by which the electronic vote and printing will be confirmed, by using bar codes (15), (16), (17) and (18) recorded on it. This ballot (13) is transferred to a second equipment (19), for the counting of the votes, where such information will be read, forming an electronic and printed storage system, in total interaction and subject to being audited, in case of concerns regarding fraud, providing total security to the electoral system.



UNITED STATES
ELECTION
ASSISTANCE
COMMISSION

2 0 0 5

VOLUNTARY VOTING SYSTEM GUIDELINES

:: Volume I :: Version 1.0

www.eac.gov

VOLUNTARY VOTING SYSTEM GUIDELINES

[Intentionally left blank]

Voluntary Voting System Guidelines

Table of Contents

Volume I Voting System Performance Guidelines

Overview	Voluntary Voting System Guidelines Overview
Section 1	Introduction
Section 2	Functional Requirements
Section 3	Usability and Accessibility Requirements
Section 4	Hardware Requirements
Section 5	Software Requirements
Section 6	Telecommunications Requirements
Section 7	Security Requirements
Section 8	Quality Assurance Requirements
Section 9	Configuration Management Requirements
Appendix A	Glossary
Appendix B	References
Appendix C	Independent Verification Systems
Appendix D	Technical Guidance for Color, Contrast, and Text Size

Volume II National Certification Testing Guidelines

Overview	Voluntary Voting System Guidelines Overview
Section 1	Introduction
Section 2	Description of the Technical Data Package
Section 3	Functionality Testing
Section 4	Hardware Testing
Section 5	Software Testing
Section 6	System Integration Testing
Section 7	Quality Assurance Testing
Appendix A	National Certification Test Plan
Appendix B	National Certification Test Report
Appendix C	National Certification Test Design Criteria

[Intentionally left blank]

VOLUNTARY VOTING SYSTEM GUIDELINES

Volume I

Voting System Performance Guidelines

[Intentionally left blank]

Voluntary Voting System Guidelines Overview

Table of Contents

Voluntary Voting System Guidelines Overview	ix
Purpose and Scope of the <i>Guidelines</i>	x
Effective Date	x
Summary of Changes.....	x
Volume I: <i>Voting System Performance Guidelines</i> Summary.....	xi
Volume II: <i>National Certification Testing Guidelines</i> Summary.....	xii
Guide to Section Locations.....	xiii

[Intentionally left blank]

Voluntary Voting System Guidelines Overview

The United States Congress passed the Help America Vote Act of 2002 (HAVA) to modernize the administration of federal elections, marking the first time in our nation's history that the federal government has funded an election reform effort. HAVA provides federal funding to help the states meet the law's uniform and non-discretionary administrative requirements, which include the following new programs and procedures: 1) provisional voting, 2) voting information, 3) statewide voter registration lists and identification requirements for first-time registrants, 4) administrative complaint procedures, and 5) updated and upgraded voting equipment.

HAVA also established the U.S. Election Assistance Commission (EAC) to administer the federal funding and to provide guidance to the states in their efforts to comply with the HAVA administrative requirements. Section 202 directs the EAC to adopt voluntary voting system guidelines, and to provide for the testing, certification, decertification, and recertification of voting system hardware and software. The purpose of the guidelines is to provide a set of specifications and requirements against which voting systems can be tested to determine if they provide all the basic functionality, accessibility, and security capabilities required of voting systems.

This document, the *Voluntary Voting System Guidelines* (referred to herein as the *Guidelines* and/or *VVSG*), is the third iteration of national level voting system standards that has been developed. The Federal Election Commission published the *Performance and Test Standards for Punchcard, Marksense and Direct Recording Electronic Voting Systems* in 1990. This was followed by the *Voting Systems Standards* in 2002.

As required by HAVA, the EAC formed the Technical Guidelines Development Committee (TGDC) to develop an initial set of recommendations for the *Guidelines*. This committee of 15 experts began their work in July 2004 and submitted their recommendations to the EAC in the 9-month timeline prescribed by HAVA. The TGDC was provided with technical support by the National Institute for Standards and Technology (NIST), which was given nearly \$3 million dollars by the EAC to complete this work.

The EAC reviewed and revised the TGDC recommendations and, as required by HAVA, published the proposed *Guidelines* for a 90 day public comment period. The document was also provided to both the Board of Advisors and the Standards Board for their review and comment. During the comment period the EAC conducted 3 public hearings on the *Guidelines* in New York City, Pasadena and Denver. Over 6000 comments were received from the public and the Boards. Each of these comments was reviewed and considered by the EAC in consultation with NIST in the development of this final version.

Purpose and Scope of the *Guidelines*

The purpose of the *Voluntary Voting System Guidelines* is to provide a set of specifications and requirements against which voting systems can be tested to determine if they provide all the basic functionality, accessibility and security capabilities required to ensure the integrity of voting systems. The *VVSG* specifies the functional requirements, performance characteristics, documentation requirements, and test evaluation criteria for the national certification of voting systems. The *VVSG* is composed of two volumes: Volume I, *Voting System Performance Guidelines* and Volume II, *National Certification Testing Guidelines*.

Effective Date

The 2005 *Voluntary Voting System Guidelines* will take effect 24 months after their final adoption in December 2005 by the EAC. At that time, all new systems submitted for national certification will be tested for conformance with these guidelines. In addition, if a modification to a system qualified or certified to a previous standard is submitted for national certification after this date, every component of the modified system will be tested against the 2005 *VVSG*. All previous versions of national standards will become obsolete at this time. This effective date provision does not have any impact on the mandatory January 1, 2006, deadline for states to comply with the HAVA Section 301 requirements.

Summary of Changes

Volume I of the *Guidelines*, entitled *Voting System Performance Guidelines*, includes new requirements for usability, accessibility, voting system software distribution, generation of software reference information, validation of software during voting system setup, and the use of wireless communications. System functional requirements have been revised to comply with HAVA Section 301 requirements. Environmental criteria have been updated. This volume also includes requirements for a voter verifiable paper audit trail component for direct-recording electronic voting systems for use by states that require this feature. In addition, this volume includes an updated glossary and a conformance clause.

Volume II of the *Guidelines*, entitled *National Certification Testing Guidelines*, has been revised to reflect the new EAC process for national certification of voting systems. This process was initiated in 2005 and replaces the voting system qualification process conducted by the National Association of State Election Directors (NASD) since 1994. In addition, revisions have been made to the testing procedures to reflect new requirements for the conduct of usability and accessibility testing. Volume II also includes an updated appendix on procedures for testing system error rates. Terminology in both volumes has been revised to reflect new terminology introduced by HAVA.

Volume I: Voting System Performance Guidelines Summary

Volume I, the *Voting System Performance Guidelines*, describes the requirements for the electronic components of voting systems. It is intended for use by the broadest audience, including voting system developers, manufacturers and suppliers; voting system testing labs; state organizations that certify systems prior to procurement; state and local election officials who procure and deploy voting systems; and public interest organizations that have an interest in voting systems and voting system standards. It contains the following sections:

Section I describes the purpose and scope of the *Voting System Performance Guidelines*.

Section 2 describes the functional capabilities required of voting systems. This section has been revised to reflect HAVA Section 301 requirements.

Section 3 describes new standards that make voting systems more usable and accessible for as many eligible citizens as possible, whatever their physical abilities, language skills, or experience with technology. This section reflects the HAVA 301 (a)(3) accessibility requirements.

Sections 4 through 6 describe specific performance standards for election system hardware, software, telecommunications, and security. Environmental criteria have been updated in Section 4.

Section 7 describes voting system security requirements and includes new requirements for voting system software distribution, generation of software reference information, validation of software during system setup, and the use of wireless. It also includes requirements for voter verifiable paper audit trail components for direct-recording electronic voting systems.

Sections 8 and 9 describe requirements for vendor quality assurance and configuration management practices and the documentation about these practices required for the EAC certification process.

Appendix A contains a glossary of terms.

Appendix B provides a list of related standards documents incorporated into the *Guidelines* by reference, documents used in the preparation of the *Guidelines*, and referenced legislation.

Appendix C presents an introductory discussion of independent verification systems as a potential concept for future voting system security design.

Appendix D contains technical guidance on color, contrast and text size adjustment for individuals with low vision or color blindness.

Volume II: *National Certification Testing Guidelines* Summary

Volume II, the *National Certification Testing Guidelines*, is a complementary document to Volume I. Volume II provides an overview and specific detail of the national certification testing process, which is performed by independent voting system test labs accredited by the EAC. It is intended principally for use by vendors; test labs; and election officials who certify, procure, and accept voting systems. This volume contains the following sections:

Section 1 describes the purpose of the *National Certification Testing Guidelines*.

Section 2 provides a description of the Technical Data Package that vendors are required to submit with their system for certification testing.

Section 3 describes the basic functionality testing requirements.

Sections 4 through 6 define the requirements for hardware, software and system integration testing. Section 6 has been revised to reflect new requirements for usability and accessibility testing.

Section 7 describes the required examination of vendor quality assurance and configuration management practices.

Appendix A provides the requirements for the National Certification Test Plan that is prepared by the voting system test lab and provided to the EAC for review.

Appendix B describes the scope and content of the National Certification Test Report which is prepared by the test lab and delivered to the EAC along with a recommendation for certification.

Appendix C describes the guiding principles used to design the voting system certification testing process. It also contains a revised section on testing system error rates.

Volume I: Voting System Performance Guidelines

Guide to Section Locations

Section 1: Introduction.....	1
Section 2: Functional Requirements	17
Section 3: Usability and Accessibility Requirements	43
Section 4: Hardware Requirements	65
Section 5: Software Requirements.....	89
Section 6: Telecommunications Requirements.....	103
Section 7: Security Requirements.....	111
Section 8: Quality Assurance Requirements.....	145
Section 9: Configuration Management Requirements.....	151
Appendix A: Glossary.....	A-1
Appendix B: References	B-1
Appendix C: Independent Verification Systems.....	C-1
Appendix D: Technical Guidance for Color, Contrast, and Text Size	D-1

[Intentionally left blank]

1 Introduction

Table of Contents

1	Introduction.....	3
1.1	Purpose and Scope of the <i>Voluntary Voting System Guidelines</i>....	3
1.2	Use of the <i>Voluntary Voting System Guidelines</i>	4
1.3	Evolution of Voting System Standards.....	5
1.3.1	Federal Election Commission.....	5
1.3.2	Election Assistance Commission.....	5
1.4	Overview of Voting System Testing.....	6
1.4.1	The National Certification Program for Voting Systems	6
1.4.2	State Certification Testing.....	7
1.4.3	Acceptance Testing	8
1.5	Definitions, References, and Types of Voting Systems	8
1.5.1	Definitions and References.....	8
1.5.2	Types of Voting Systems.....	9
1.5.2.1	Paper-Based Voting System	10
1.5.2.2	Direct-Recording Electronic Voting System	10
1.5.2.3	Public Network Direct-Recording Electronic Voting System ..	10
1.5.2.4	Precinct Count Voting System.....	11
1.5.2.5	Central Count Voting System	11
1.6	Conformance Clause	11
1.6.1	Scope and Applicability	11
1.6.2	Conformance Framework.....	12
1.6.2.1	Applicable Entities.....	12
1.6.2.2	Relationships Among Entities	13
1.6.3	Structure of Requirements.....	13
1.6.3.1	Conformance Language.....	14
1.6.3.2	Categorizing Requirements	14
1.6.3.3	Extensions.....	15
1.6.4	Implementation Statement.....	15
1.7	Effective Date	15

[Intentionally left blank]

1 Introduction

1.1 Purpose and Scope of the *Voluntary Voting System Guidelines*

The purpose of the *Voluntary Voting System Guidelines* (VMSG or the *Guidelines*) is to provide a set of specifications and requirements against which voting systems can be tested to determine if they provide all the basic functionality, accessibility, and security capabilities required of voting systems. The VMSG specifies the functional requirements, performance characteristics, documentation requirements, and test evaluation criteria for the national certification of voting systems. To the extent possible, these requirements and specifications are described so they can be assessed by a series of defined, objective tests. The VMSG is composed of two volumes: Volume 1, *Voting System Performance Guidelines*; and Volume 2, *National Certification Testing Guidelines*.

The VMSG is one of several inter-related EAC promulgated guidelines and programs concerned with maintaining the reliability and security of voting systems and the integrity of the overall election process. The performance of national certification testing of voting systems is restricted to testing labs that have been formally accredited to be technically competent to evaluate systems for conformance to the *Voting System Performance Guidelines*. The National Association of State Election Directors (NASED) initiated the independent testing authority accreditation program for test labs in 1994, applying the standards and procedures in NASSED Program Handbook 9201 (Revision A). With the passage of the Help America Vote Act (HAVA), this responsibility transitioned to the Election Assistance Commission (EAC) with support from the National Voluntary Laboratory Accreditation Program (NVLAP). This program is operated by the National Institute of Standards and Technology (NIST), applying the standards and procedures in NIST Handbook 150-22, NVLAP Voting System Testing.

The VMSG and the test lab accreditation process are essential components of the EAC National Certification Program for voting systems. This program applies the standards and procedures documented in the EAC voting system certification manual. HAVA Section 231 charges EAC with providing for the certification, decertification and recertification of voting systems. Under this program national certification is just the first step of the life cycle process of maintaining the reliability and security of the voting systems used in the nation's elections. To carry out this mandate, the EAC program will include monitoring of voting system performance through incident reporting by election officials and others. The certification program will maintain information on the quality assurance practices associated with the development and manufacturing of voting systems. When a system has successfully completed the certification process, the EAC program requires a copy of the certified voting system software to be provided to the National Software Reference Library operated by NIST. This will enable election officials to validate that the software received by their jurisdictions is the same as the certified version.

The VMSG notes the need for appropriate procedures to complement and supplement the technical requirements for voting system performance. It is well known that deficiencies in

election management and administration procedures can have just as much impact on the enfranchisement of voters and the outcome of elections as the functioning of the voting machines. The overall integrity of the election process depends on both of these elements working together. EAC and NASED have instituted a multi-year effort to develop a comprehensive set of election management guidelines that will complement the technical system guidelines, as well as cover other elements of the election process.

Except as noted below, Volume I of the *Guidelines* applies to all system hardware, software, telecommunications, and documentation intended for use to:

- Prepare the voting system for use in an election
- Produce the appropriate ballot formats
- Test that the voting system and ballot materials have been properly prepared and are ready for use
- Record and count votes
- Consolidate and report election results
- Display results on-site or remotely
- Produce and maintain comprehensive audit trail data

Some voting systems use one or more commercial off-the-shelf (COTS) devices (such as card readers, printers, and personal computers) or software products (such as operating systems, programming language compilers, and database management systems). These devices and products are exempt from certain portions of system certification testing, as long as they are not modified for use in the voting system.

Volume 2 describes the testing process to provide a documented independent verification by an accredited testing laboratory that a voting system has been demonstrated to conform to the Volume 1 requirements and therefore should receive national certification. It provides the specific detail about the testing process and documentation requirements required to support the national certification program.

1.2 Use of the *Voluntary Voting System Guidelines*

The *Guidelines* are intended for use by multiple audiences to support their respective roles in the development, testing, and acquisition of voting systems:

- The accredited testing laboratories who use this information to develop test plans and procedures for the analysis and testing of systems in support of the national certification testing process
- State and local election officials who are evaluating voting systems for potential use in their jurisdictions
- Voting system designers and manufacturers who need to ensure that their products fulfill all these requirements so they can be certified

1.3 Evolution of Voting System Standards

1.3.1 Federal Election Commission

The first voting system standards were issued in January 1990, by the Federal Election Commission (FEC). This document included performance standards and testing procedures for Punchcard, Marksense, and Direct-Recording Electronic (DRE) voting systems. These standards did not cover paper ballot and mechanical lever systems because paper ballots are sufficiently self-explanatory not to require technical standards and mechanical lever systems are no longer manufactured or sold in the United States. The FEC also did not incorporate requirements for mainframe computer hardware because it was reasonable to assume that sufficient engineering and performance criteria already governed the operation of mainframe computers. However, vote tally software installed on mainframes was covered.

A national testing effort was initiated by NASED in 1994. As the system qualification process matured and qualified systems were used in the field, the NASED Voting Systems Board, in consultation with the testing labs, identified certain testing issues that needed to be resolved. Moreover, rapid advancements in information and personal computer technologies introduced new voting system development and implementation scenarios not contemplated by the 1990 Standards.

In 1997, NASED briefed the FEC on the importance of keeping the Standards up to date. Following a requirements analysis completed in 1999, the FEC initiated an effort to revise the 1990 Standards to reflect the evolving needs of the elections community. This resulted in the 2002 Voting Systems Standards.

Voters and election officials who use voting systems represent a broad spectrum of the population, and include individuals with disabilities who may have difficulty using traditional voting systems. In developing accessibility provisions for the 2002 Voting System Standards, the FEC requested assistance from the Access Board, the federal agency in the forefront of promulgating accessibility provisions. The Access Board submitted technical standards to meet the diverse needs of voters with a broad range of disabilities. The FEC adopted the entirety of the Access Board's recommendations and incorporated them into the 2002 Voting Systems Standards.

1.3.2 Election Assistance Commission

In 2002, Congress passed the Help America Vote Act, which established the U.S. Election Assistance Commission (EAC). EAC was mandated to develop and adopt new voluntary voting system guidelines and to provide for the testing, certification, and decertification of voting systems. HAVA also established the Technical Guidelines Development Committee (TGDC) with the duty of assisting the EAC in the development of the new guidelines. The Director of NIST chairs the TGDC, and NIST was tasked to provide technical support to their work. The TGDC delivered their initial set of recommendations to the EAC in May, 2005.

The TGDC built on the foundation of the 2002 Voting Systems Standards and the accessibility provisions of HAVA to expand requirements for voting system usability and accessibility. HAVA mandates that voting systems shall be accessible for individuals with disabilities in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters. To facilitate the ability of jurisdictions to meet these requirements, HAVA allows for the use of at least one direct-recording electronic or other voting system equipped for individuals with disabilities at each polling place. Implementing this provision, however, will not entirely eliminate the necessity of accommodating the needs of some disabled voters by human assistance, given the limitations of current technology.

The 2005 *VVSG* is the culmination of sixteen months of effort by the TGDC, NIST and the EAC. There is still much to be done to further develop the technical guidelines for voting system performance, accessibility and usability features, and security. Further work is also needed for the specification of comprehensive standard test suites for certification testing, to include testing for usability and accessibility features and expanded security testing.

1.4 Overview of Voting System Testing

1.4.1 The National Certification Program for Voting Systems

The purpose of the national certification program is to validate and document, through an independent testing process, that voting systems meet the requirements set forth in *VVSG* Volume 1 - *Voting System Performance Guidelines*, and perform according to the vendor's specifications for the system. Volume 1 specifies the minimum functional requirements, performance characteristics, documentation requirements, and test evaluation criteria that voting systems must meet in order to receive national certification. At the time of *VVSG* 2005 publication, 39 states either require national certification or utilize the national standards when certifying voting systems.

National certification testing can only be performed by testing labs that have been accredited for demonstrated technical competence to test voting systems using these *Guidelines*. Volume 2 of the *VVSG - National Certification Testing Guidelines* - provides guidance on the testing process and describes the associated documentation requirements. These tests encompass the examination of software; the inspection and evaluation of system documentation; tests of hardware under conditions simulating the intended storage, operation, transportation, and maintenance environments; operational tests to validate system performance and function under normal and abnormal conditions; and examination of the vendor's system development, testing, quality assurance, and configuration management practices. Certification tests address individual system components or elements, as well as the integrated system as a whole.

Since 1994, testing of voting systems has been performed by Independent Test Authorities (ITAs) certified by NASED. Upon the successful completion of testing, the ITA issued a Qualification Test Report to the vendor and NASED. The Technical Committee of the

NASED Voting Systems Board would review the test report and, if satisfactory, issue a Qualification Number. The Qualification Number remains valid for as long as the voting system remains unchanged.

HAVA mandated that the certification testing process be transferred from NASED to EAC. National certification testing complements and evaluates the vendor's developmental testing and beta testing. The test lab is expected to evaluate the completeness of the vendor's developmental test program, including the sufficiency of vendor tests conducted to demonstrate compliance with the *Guidelines* as well as the system's performance specifications. The test lab undertakes sample testing of the vendor's test modules and also designs independent system-level tests to supplement and check those designed by the vendor. Although some of the certification tests are based on those prescribed in the Military Standards, in most cases the test conditions are less stringent, reflecting commercial, rather than military, practice.

Upon review of test reports and a determination that satisfactory results were achieved that address the full scope of testing, EAC will issue a certification number that indicates the system has successfully completed testing by an accredited test lab for compliance with the *Guidelines*. The certification number applies to the system as a whole and does not apply to individual system components or untested configurations.

After a system has completed initial certification testing, further examination of the system is required if modifications are made to hardware, software, or telecommunications, including the installation of software on different hardware. Vendors request review of modifications by the test lab based on the nature and scope of changes made. The test lab will assess whether the modified system should be resubmitted for certification testing and the extent of testing to be conducted, and then it will provide an appropriate recommendation to the EAC and the vendor.

Generally, a voting system remains certified under the standards against which it was tested as long as no modifications requiring recertification have been made to the system. However, if a new threat to a particular voting system is discovered, it is the prerogative of EAC to determine which certified voting systems are vulnerable, whether those systems need to be retested, and the specific tests to be conducted. In addition, when new requirements supersede the requirements under which the system was certified, it is the prerogative of EAC to determine when systems that were certified under the earlier requirements will need to be re-tested to meet current guidelines.

1.4.2 State Certification Testing

State certification tests are performed by individual states, with or without the assistance of outside consultants, to:

- Confirm that the voting system presented is the same as the one certified under the *Guidelines*

- Test for the proper implementation of state-specific requirements
- Establish a baseline for future evaluations or tests of the system, such as acceptance testing or state review after modifications have been made
- Define acceptance tests

State certification test scripts are not included in the *Guidelines*, as they must be defined by the state, with its laws, election practices, and needs in mind. However, it is recommended that they not duplicate the national certification tests, but instead focus on functional tests and qualitative assessment to ensure that the system operates in a manner that is acceptable under state law. If a voting system is modified after state certification is completed, it is recommended that states reevaluate the system to determine if further certification testing is warranted.

Certification tests performed by individual states typically rely on information contained in documentation provided by the vendor for system design, installation, operations, required facilities and supplies, personnel support and other aspects of the voting system. States and jurisdictions may define information and documentation requirements additional to those defined in the *Guidelines*. By design, the *Guidelines* do not address these additional requirements. However, national certification testing will address all the capabilities of a voting system stated by the vendor in the system documentation submitted with the testing application to the EAC, including additional capabilities that are not required by the states.

1.4.3 Acceptance Testing

Acceptance tests are performed at the state or local jurisdiction level upon system delivery by the vendor to:

- Confirm that the system delivered is the specific system certified by EAC and, when applicable, certified by the state
- Evaluate the degree to which delivered units conform to both the system characteristics specified in the procurement documentation, and those demonstrated in the national and state certification tests
- Establish a baseline for any future required audits of the system

Some of the operational tests conducted during certification may be repeated during acceptance testing.

1.5 Definitions, References, and Types of Voting Systems

1.5.1 Definitions and References

The *Guidelines* contain terms describing function, design, documentation, and testing attributes of voting system hardware, software and telecommunications. Unless otherwise specified, the intended sense of technical terms is that which is commonly used by the

information technology industry. In some cases terminology is specific to elections or voting systems. A glossary of terms is contained in Appendix A. Non-technical terms not listed in Appendix A shall be interpreted according to their standard dictionary definitions.

There are a number of technical standards that are incorporated in the *Guidelines* by reference. These are referred to by title in the body of the document. The full citations for these publications are provided in Appendix B. In addition, this appendix includes other references that may be useful for understanding and interpretation.

1.5.2 Types of Voting Systems

HAVA Section 301 defines a voting system as the total combination of mechanical, electromechanical, or electronic equipment (including the software, firmware, and documentation required to program, control, and support the equipment), that is used to define ballots; to cast and count votes; to report or display election results; and to maintain and produce any audit trail information. In addition, a voting system includes the practices and associated documentation used to identify system components and versions of such components; to test the system during its development and maintenance; to maintain records of system errors and defects; to determine specific system changes made after initial certification; and to make available any materials to the voter (such as notices, instructions, forms, or paper ballots).

Traditionally, a voting system has been defined by the mechanism the system uses to cast votes and further categorized by the location where the system tabulates ballots. In addition to defining a common set of requirements that apply to all voting systems, the *VVSG* states requirements specific to a particular type of voting system, where appropriate. However, the *Guidelines* recognize that as the industry develops new solutions and the technology continues to evolve, the distinctions between voting system types may become blurred. The fact that the *VVSG* refers to specific system types is not intended to stifle innovations that may be based on a more fluid understanding of system types. However, appropriate procedures must be in place to ensure new developments provide the necessary integrity and can be properly evaluated in the certification process.

Consequently, vendors that submit a system that integrates components from more than one traditional system type or a system that includes components or technology not addressed in the *Guidelines* shall submit the results of all beta tests of the new system when applying for national certification. Vendors shall also submit a proposed test plan to the EAC for use in national certification testing. The *Guidelines* permit vendors to produce or utilize interoperable components of a voting system that are tested within the full voting system configuration.

The listing below summarizes the functional requirements that HAVA Section 301 mandates to assist voters. While these requirements may be implemented in a different manner for different types of voting systems, all types of voting systems must provide these capabilities:

- permit the voter to verify (in a private and independent manner) the vote selected by the voter on the ballot before the ballot is cast and counted
- provide the voter with the opportunity (in a private and independent manner) to change the ballot or correct any error before the ballot is cast and counted
- notify the voter if he or she has selected more than one candidate for a single office, inform the voter of the effect of casting multiple votes for a single office, and provide the voter an opportunity to correct the ballot before it is cast and counted
- be accessible for individuals with disabilities in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters
- provide alternative language accessibility pursuant to Section 203 of the Voting Rights Act

1.5.2.1 Paper-Based Voting System

A paper-based voting system records votes, counts votes, and produces a tabulation of the vote count from votes cast on paper cards or sheets. A marksense (also known as optical scan) voting system allows a voter to record votes by making marks directly on the ballot, usually in voting response locations. Additionally, a paper-based system may allow for the voter's selections to be indicated by marks made on a paper ballot by an electronic input device, as long as such an input device does not independently record, store, or tabulate the voter selections.

1.5.2.2 Direct-Recording Electronic Voting System

A direct-recording electronic (DRE) voting system records votes by means of a ballot display provided with mechanical or electro-optical components that can be activated by the voter; that processes data by means of a computer program; and that records voting data and ballot images in memory components. It produces a tabulation of the voting data stored in a removable memory component and as printed copy. The system may also provide a means for transmitting individual ballots or vote totals to a central location for consolidating and reporting results from precincts at the central location.

1.5.2.3 Public Network Direct-Recording Electronic Voting System

A public network DRE voting system is an election system that uses electronic ballots and transmits vote data from the polling place to another location over a public network. Vote data may be transmitted as individual ballots as they are cast, periodically as batches of ballots throughout the election day, or as one batch at the close of voting. For purposes of the *Guidelines*, public network DRE voting systems are considered a form of DRE voting system and are subject to the standards applicable to DRE voting systems. However, because transmitting vote data over public networks relies on equipment beyond the control of the

election authority, the system is subject to additional threats to system integrity and availability. Therefore, additional requirements are applied to provide appropriate security for data transmission.

The use of public networks for transmitting vote data must provide the same level of integrity as other forms of voting systems, and must be accomplished in a manner that precludes three risks to the election process: automated casting of fraudulent votes, automated manipulation of vote counts, and disruption of the voting process such that the system is unavailable to voters during the time period authorized for system use.

1.5.2.4 Precinct Count Voting System

A precinct count voting system is a voting system that tabulates ballots at the polling place. These systems typically tabulate ballots as they are cast and print the results after the close of polling. For DREs and some paper-based systems these systems provide electronic storage of the vote count and may transmit results to a central location over public telecommunication networks.

1.5.2.5 Central Count Voting System

A central count voting system is a voting system that tabulates ballots from multiple precincts at a central location. Voted ballots are typically placed into secure storage at the polling place. Stored ballots are transported or transmitted to a central counting location. The system produces a printed report of the vote count, and may produce a report stored on electronic media.

1.6 Conformance Clause

1.6.1 Scope and Applicability

The *Voluntary Voting System Guidelines* define requirements for conformance of voting systems that voting system vendors shall meet. The *Guidelines* also provide the framework, procedures, and requirements that testing labs responsible for the certification testing of voting systems shall follow. The requirements and procedures in the *Guidelines* may also be used by states to certify voting systems. To ensure that correct voting system software has been distributed without modification, the *Guidelines* include requirements for certified voting system software to be deposited in a national software repository. This provides an independent means for election officials to verify the software they purchase.

The *Guidelines* define the minimum requirements for voting systems and the process of testing voting systems. The guidelines are intended for use by:

- Designers and manufacturers of voting systems
- Test labs performing the analysis and testing of voting systems in support of the EAC national certification process
- Software repositories designated by EAC or by a state
- Election officials, including ballot designers and officials responsible for the installation, operation, and maintenance of voting machines
- Test labs and consultants performing the state certification of voting systems

Minimum requirements specified in these guidelines include:

- Functional capabilities
- Performance characteristics, including security
- Documentation
- Test evaluation criteria

1.6.2 Conformance Framework

This section provides the framework in which conformance is defined. It identifies the entities to which these guidelines apply, the relationships among the various entities, the structure of the requirements, and the terminology used to indicate conformance.

1.6.2.1 Applicable Entities

The requirements, prohibitions, options, and guidance specified in these guidelines apply to voting systems, voting system vendors, test labs, and software repositories. In general, requirements for voting systems in these guidelines apply to all types of voting systems, unless prefaced with explanatory narrative that applicability is limited to a specific type of system. Other terms in these guidelines shall be construed as synonymous with “voting systems.” They are: “systems”, “the system”, “the voting system”, and “each voting system.”

The term “voting system vendor” imposes documentation or testing requirements for the manufacturer or vendor. Other terms in these guidelines shall be construed as synonymous with “voting system vendor.” They are: “vendors”, “the vendor”, “manufacturer or vendor”, “voting system designers”, and “implementer”.

The terms used to designate requirements and procedural guidelines for national certification testing laboratories are indicated by referring to “testing authorities”, “test labs”, and “accredited test labs”. The term “repository” will be used to designate requirements levied on the National Software Reference Library repository maintained at NIST or any other designated repository.

1.6.2.2 Relationships Among Entities

It is the voting system vendor that needs to implement these requirements and provide the necessary documentation for the system. In order to claim conformance to the *Guidelines*, the voting system vendor shall satisfy the specified requirements, including implementation of functionality, prescribed software coding and assurance practices, and preparation of the Technical Data Package. The voting system vendor shall successfully complete the prescribed test campaign with an EAC accredited test lab.

The accredited test lab shall satisfy the requirements for conducting certification testing. The test lab may use an operational environment emulating that used by election officials as part of their testing to ensure that the voting system can be configured and operated in a secure and reliable manner according to the vendor's documentation and as specified by the *Guidelines*. The test lab shall coordinate and deliver the requisite documentation and test report to the EAC for review. Upon issuance of a certification number by the EAC, the test lab shall deposit a copy of the certified voting system software with the National Software Reference Library.

The EAC shall review the test results and associated documentation and make a determination that all requirements have been appropriately tested and the test results are acceptable. The EAC will issue a national certification number that indicates conformance of the specified system with these *Guidelines*.

The National Software Reference Library (NSRL) shall create a digital signature of the voting system software provided by the test lab. This information will be posted to a website so election officials can compare the digital signature of the software provided to them by the voting system vendor with this certified reference. The NSRL shall maintain this reference information until notified by the EAC that it can be archived.

1.6.3 Structure of Requirements

Each voting system requirement in Volume I is identified according to a hierarchical scheme in which higher-level requirements (such as “provide accessibility for visually impaired voters”) are supported by lower-level requirements (e.g., “provide an audio-tactile interface”). Thus, requirements are nested. When the nesting hierarchy has reached four levels (i.e., 1.1.1.1), further nested requirements are designated with lowercase letters, then roman numerals. Therefore, all requirements are traceable by a distinct reference.

Some requirements are directly testable and some are not. The latter tend to be higher-level and are included because (1) they are testable indirectly insofar as their lower-level requirements are testable, and (2) they often provide the structure and rationale for the lower-level requirements. Satisfying the lower-level requirements will result in satisfying the higher-level requirement.

1.6.3.1 Conformance Language

The following keywords are used to convey conformance requirements:

- **Shall** – indicates a mandatory requirement in order to conform. Synonymous with “is required to.”
- **Is prohibited** – indicates a mandatory requirement that indicates something that is not permitted (allowed) in order to conform. Synonymous with “shall not.”
- **Should, is encouraged** - indicates an optional recommended action, one that is particularly suitable, without mentioning or excluding others. Synonymous with “is permitted and recommended.”
- **May** - indicates an optional, permissible action. Synonymous with “is permitted.”

Informative parts of this document include examples, extended explanations, and other matter that contain information necessary for proper understanding of the *Guidelines* and conformance to it.

1.6.3.2 Categorizing Requirements

The *Guidelines* set forth a common set of requirements for national certification that apply to all types of electronic voting systems. They also provide requirements that are applicable for particular circumstances, such as alternative language capability or disability accessibility. The requirements implementing the HAVA Section 301(a) mandates, except for disability accessibility, must be met by all voting systems. The alternative language capability mandated by Section 301(a)(4) must be met by all systems intended for use in jurisdictions subject to Section 203 of the Voting Rights Act. The Section 301(a)(3) disability accessibility requirements must be met by all systems intended to fulfill the one per polling place disability equipped voting system provision of Section 301(a)(3)(B).

In addition, the *Guidelines* categorize some requirements into related groups of functionality to address equipment type, ballot tabulation location, and voting system component (e.g., election management system, voting machine). Hence, all of the requirements contained in the *Guidelines* do not apply to all elements of all voting systems. For example, requirements categorized as applying to DRE systems are not applicable to paper-based voting. The requirements implementing disability accessibility are not required of all voting systems, only by those systems the vendor designates as accessible voting systems.

Among the categories defined in the *VVSG* are two types of voting systems with respect to mechanisms to cast votes – paper-based voting systems and DRE voting systems. Additionally, voting systems are further categorized by the locations where ballots are tabulated – precinct count voting systems, which tabulate ballots at the polling place, and central count voting systems, which tabulate ballots from multiple precincts at a central location. The *Guidelines* define specific requirements for systems that fall within these four categories as well as various combinations of these categories.

1.6.3.3 Extensions

Extensions are additional functions, features, and/or capabilities included in a voting system that are not required by the *Guidelines*. To accommodate the needs of states that may impose additional requirements and to accommodate changes in technology, these guidelines allow extensions. For example, the requirements for a voter verifiable paper audit trail feature will only be applied to those systems designated by the vendor as providing this feature. The use of extensions shall not contradict nor cause the nonconformance of functionality required by the *Guidelines*.

1.6.4 Implementation Statement

The voting system implementation statement describes the voting system and documents the *VVSG* Volume 1 requirements that have been implemented by the voting system. It can also identify optional features and capabilities supported by the voting system, as well as any extensions (i.e., additional functionality beyond what is required in the guidelines). The implementation statement must include a checklist identifying all the requirements for which a claim of conformance is made.

The implementation statement must be submitted with the vendor's application to the EAC for national certification testing. It must provide a concise summary and narrative description of the voting system's capabilities. It shall include identifying information about the voting system, including the hardware and software components, version number and date.

1.7 Effective Date

The *Voluntary Voting System Guidelines (VVSG)* shall become effective for national certification testing 24 months after their final adoption in December, 2005 by EAC. At that time, all new systems submitted for national certification shall be tested for conformance with these *Guidelines*. In addition, if a modification to a system certified or qualified to a previous standard is submitted for national certification after this date, every component of the modified system shall be tested using these *Guidelines*. All previous versions of national voting system standards will become obsolete upon this effective date.

These *Guidelines* are voluntary in that each of the states can decide whether to require the voting systems used in their state to have a national certification. States may decide to adopt these *Guidelines* in whole or in part at any time, irrespective of the effective date. In addition, states may specify additional requirements that voting systems in their jurisdiction must meet. The national certification program does not in any way pre-empt the ability of the states to have their own system certification process.

This *VVSG* effective date provision has no effect on the mandatory voting system requirements prescribed in HAVA Section 301(a), which states must comply with on or before January 1, 2006. The EAC issued Advisory 2005-004 to assist states in determining if

a voting system is compliant with Section 301(a). This advisory is available on the EAC website at www.eac.gov.

2 Functional Requirements

Table of Contents

2	Functional Requirements	19
2.1	Overall System Capabilities	19
2.1.1	Security	20
2.1.2	Accuracy	21
2.1.3	Error Recovery	21
2.1.4	Integrity	22
2.1.5	System Audit	22
2.1.5.1	Operational Requirements	23
2.1.5.2	Use of Shared Computing Platforms	25
2.1.6	Election Management System	26
2.1.7	Vote Tabulating Program	26
2.1.7.1	Functions.....	26
2.1.7.2	Voting Variations.....	27
2.1.8	Ballot Counter	27
2.1.9	Telecommunications.....	28
2.1.10	Data Retention	28
2.2	Pre-voting Capabilities	29
2.2.1	Ballot Preparation	29
2.2.1.1	General Capabilities.....	30
2.2.1.2	Ballot Formatting.....	30
2.2.1.3	Ballot Production	31
2.2.2	Election Programming.....	31
2.2.3	Ballot and Program Installation and Control.....	32
2.2.4	Readiness Testing.....	32
2.2.5	Verification at the Polling Place.....	33
2.2.6	Verification at the Central Location	34
2.3	Voting Capabilities	34
2.3.1	Opening the Polls	35
2.3.1.1	Precinct Count Systems	35
2.3.1.2	Paper-based System Requirements.....	35
2.3.1.3	DRE System Requirements	35
2.3.2	Activating the Ballot (DRE Systems).....	36
2.3.3	Casting a Ballot	36
2.3.3.1	Common Requirements	36
2.3.3.2	Paper-based System Requirements.....	37
2.3.3.3	DRE System Requirements	38
2.4	Post-Voting Capabilities	39
2.4.1	Closing the Polls.....	39
2.4.2	Consolidating Vote Data	40

2.4.3	Producing Reports	40
2.4.4	Broadcasting Results	41
2.5	Maintenance, Transportation, and Storage	41

2 Functional Requirements

This section contains requirements detailing the functional capabilities required of a voting system. This section sets out precisely what a voting system is required to do. In addition, it sets forth the minimum actions a voting system must be able to perform to be eligible for certification.

For organizational purposes, functional capabilities are categorized as follows by the phase of election activity in which they are required:

2.1 Overall System Capabilities: These functional capabilities apply throughout the election process. They include security, accuracy, integrity, system auditability, election management system, vote tabulation, ballot counters, telecommunications, and data retention.

2.2 Pre-voting Capabilities: These functional capabilities are used to prepare the voting system for voting. They include ballot preparation, the preparation of election-specific software (including firmware), the production of ballots, the installation of ballots and ballot counting software (including firmware), and system and equipment tests.

2.3 Voting System Capabilities: These functional capabilities include all operations conducted at the polling place by voters and officials including the generation of status messages.

2.4 Post-voting Capabilities: These functional capabilities apply after all votes have been cast. They include closing the polling place; obtaining reports by voting machine, polling place, and precinct; obtaining consolidated reports; and obtaining reports of audit trails.

2.5 Maintenance, Transportation and Storage Capabilities: These capabilities are necessary to maintain, transport, and store voting system equipment.

In recognition of the diversity of voting systems, the *Guidelines* apply specific requirements to specific technologies. Some of the guidelines apply only if the system incorporates certain optional functions (for example, voting systems employing telecommunications to transmit voting data). For each functional capability, common requirements are specified. Where necessary, these are followed by requirements applicable to specific technologies (i.e., paper-based or DRE) or intended use (i.e., central or precinct count).

2.1 Overall System Capabilities

This section defines required functional capabilities that are system-wide in nature and not unique to pre-voting, voting, and post-voting operations. All voting systems shall provide the following functional capabilities, further outlined in this section:

- 2.1.1 Security
- 2.1.2 Accuracy
- 2.1.3 Error Recovery
- 2.1.4 Integrity
- 2.1.5 System Audit
- 2.1.6 Election Management System
- 2.1.7 Vote Tabulating Program
- 2.1.8 Ballot Counter
- 2.1.9 Telecommunications
- 2.1.10 Data Retention

Voting systems may also include telecommunications components. Technical standards for these capabilities are described in Sections 3 through 6 of the *Voluntary Voting System Guidelines*.

2.1.1 Security

System security is achieved through a combination of technical capabilities and sound administrative practices. To ensure security, all systems shall:

- a. Provide security access controls that limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality, and accountability
- b. Provide system functions that are executable only in the intended manner and order, and only under the intended conditions
- c. Use the system's control logic to prevent a system function from executing if any preconditions to the function have not been met
- d. Provide safeguards in response to system failure to protect against tampering during system repair or interventions in system operations
- e. Provide security provisions that are compatible with the procedures and administrative tasks involved in equipment preparation, testing, and operation
- f. Incorporate a means of implementing a capability if access to a system function is to be restricted or controlled
- g. Provide documentation of mandatory administrative procedures for effective system security

2.1.2 Accuracy

Memory hardware, such as semiconductor devices and magnetic storage media, must be accurate. The design of equipment in all voting systems shall provide for the highest possible levels of protection against mechanical, thermal, and electromagnetic stresses that impact system accuracy. Section 4 provides additional information on susceptibility requirements. To ensure vote accuracy, all systems shall:

- a. Record the election contests, candidates, and issues exactly as defined by election officials
- b. Record the appropriate options for casting and recording votes
- c. Record each vote precisely as indicated by the voter and produce an accurate report of all votes cast;
- d. Include control logic and data processing methods incorporating parity and check-sums (or equivalent error detection and correction methods) to demonstrate that the system has been designed for accuracy
- e. Provide software that monitors the overall quality of data read-write and transfer quality status, checking the number and types of errors that occur in any of the relevant operations on data and how they were corrected

In addition, DRE systems shall:

- f. As an additional means of ensuring accuracy in DRE systems, voting devices shall record and retain redundant copies of the original ballot image. A ballot image is an electronic record of all votes cast by the voter, including undervotes.

2.1.3 Error Recovery

To recover from a non-catastrophic failure of a device, or from any error or malfunction that is within the operator's ability to correct, the system shall provide the following capabilities:

- a. Restoration of the device to the operating condition existing immediately prior to the error or failure, without loss or corruption of voting data previously stored in the device
- b. Resumption of normal operation following the correction of a failure in a memory component, or in a data processing component, including the central processing unit
- c. Recovery from any other external condition that causes equipment to become inoperable, provided that catastrophic electrical or mechanical damage due to external phenomena has not occurred

2.1.4 Integrity

Integrity measures ensure the physical stability and function of the vote recording and counting processes.

To ensure system integrity, all systems shall:

- a. Protect against a single point of failure that would prevent further voting at the polling place
- b. Protect against the interruption of electrical power
- c. Protect against generated or induced electromagnetic radiation
- d. Protect against ambient temperature and humidity fluctuations
- e. Protect against the failure of any data input or storage device
- f. Protect against any attempt at improper data entry or retrieval
- g. Record and report the date and time of normal and abnormal events
- h. Maintain a permanent record of all original audit data that cannot be modified or overridden but may be augmented by designated authorized officials in order to adjust for errors or omissions (e.g., during the canvassing process)
- i. Detect and record every event, including the occurrence of an error condition that the system cannot overcome, and time-dependent or programmed events that occur without the intervention of the voter or a polling place operator
- j. Include built-in measurement, self-test, and diagnostic software and hardware for detecting and reporting the system's status and degree of operability

In addition to the common requirements, DRE systems shall:

- k. Maintain a record of each ballot cast using a process and storage location that differs from the main vote detection, interpretation, processing, and reporting path
- l. Provide a capability to retrieve ballot images in a form readable by humans

2.1.5 System Audit

This subsection describes the context and purpose of voting system audits and sets forth specific functional requirements. Election audit trails provide the supporting documentation for verifying the accuracy of reported election results. They present a concrete, indestructible archival record of all system activity related to the vote tally, and are essential for public confidence in the accuracy of the tally, for recounts, and for evidence in the event of criminal or civil litigation.

These requirements are based on the premise that system-generated creation and maintenance of audit records reduces the chance of error associated with manually generated audit records. Because most audit capability is automatic, the system operator has less information to track and record, and is less likely to make mistakes or omissions. The subsections that follow present operational requirements critical to acceptable performance and reconstruction of an election. Requirements for the content of audit records are described in Section 5.

The requirements for all system types, both precinct and central count, are described in generic language. Because the actual implementation of specific characteristics may vary from system to system, it is the responsibility of the vendor to describe each system's characteristics in sufficient detail so that test labs and system users can evaluate the adequacy of the system's audit trail. This description shall be incorporated in the System Operating Manual, which is part of the Technical Data Package.

Documentation of items such as paper ballots delivered, paper ballots collected, administrative procedures for system security, and maintenance performed on voting equipment are also part of the election audit trail, but are not covered in these technical standards. Useful guidance is provided by the *Innovations in Election Administration #10: Ballot Security and Accountability*, available on the EAC's website.

2.1.5.1 Operational Requirements

Audit records shall be prepared for all phases of election operations performed using devices controlled by the jurisdiction or its contractors. These records rely upon automated audit data acquisition and machine-generated reports, with manual input of some information. These records shall address the ballot preparation and election definition phase, system readiness tests, and voting and ballot-counting operations. The software shall activate the logging and reporting of audit data as described below.

- a. The timing and sequence of audit record entries is as important as the data contained in the record. All voting systems shall meet the requirements for time, sequence and preservation of audit records outlined below.
 - i. Except where noted, systems shall provide the capability to create and maintain a real-time audit record. This capability records and provides the operator or precinct official with continuous updates on machine status. This information allows effective operator identification of an error condition requiring intervention, and contributes to the reconstruction of election-related events necessary for recounts or litigation.
 - ii. All systems shall include a real-time clock as part of the system's hardware. The system shall maintain an absolute record of the time and date or a record relative to some event whose time and data are known and recorded.
 - iii. All audit record entries shall include the time-and-date stamp.

- iv. The audit record shall be active whenever the system is in an operating mode. This record shall be available at all times, though it need not be continually visible.
 - v. The generation of audit record entries shall not be terminated or altered by program control, or by the intervention of any person. The physical security and integrity of the record shall be maintained at all times.
 - vi. Once the system has been activated for any function, the system shall preserve the contents of the audit record during any interruption of power to the system until processing and data reporting have been completed.
 - vii. The system shall be capable of printing a copy of the audit record. A separate printer is not required for the audit record, and the record may be produced on the standard system printer if all the following conditions are met:
 - The generation of audit trail records does not interfere with the production of output reports
 - The entries can be identified so as to facilitate their recognition, segregation, and retention
 - The audit record entries are kept physically secure
- b. All voting systems shall meet the requirements for error messages below.
- i. The voting system shall generate, store, and report to the user all error messages as they occur.
 - ii. All error messages requiring intervention by an operator or precinct official shall be displayed or printed clearly in easily understood language text, or by means of other suitable visual indicators.
 - iii. When the voting system uses numerical error codes for trained technician maintenance or repair, the text corresponding to the code shall be self-contained or affixed inside the voting machine. This is intended to reduce inappropriate reactions to error conditions, and to allow for ready and effective problem correction.
 - iv. All error messages for which correction impacts vote recording or vote processing shall be written in a manner that is understandable to an election official who possesses training on system use and operation, but does not possess technical training on system servicing and repair.
 - v. The message cue for all voting systems shall clearly state the action to be performed in the event that voter or operator response is required.
 - vi. Voting system design shall ensure that erroneous responses will not lead to irreversible error.

- vii. Nested error conditions shall be corrected in a controlled sequence such that voting system status shall be restored to the initial state existing before the first error occurred.
- c. The *Guidelines* provide latitude in software design so that vendors can consider various user processing and reporting needs. The jurisdiction may require some status and information messages to be displayed and reported in real-time. Messages that do not require operator intervention may be stored in memory to be recovered after ballot processing has been completed.

The voting system shall display and report critical status messages using clear indicators or English language text. The voting system need not display non-critical status messages at the time of occurrence. Voting systems may display non-critical status messages (i.e., those that do not require operator intervention) by means of numerical codes for subsequent interpretation and reporting as unambiguous text.

Voting systems shall provide a capability for the status messages to become part of the real-time audit record. The voting system shall provide a capability for a jurisdiction to designate critical status messages.

2.1.5.2 Use of Shared Computing Platforms

Further requirements must be applied to Commercial-off-the-Shelf operating systems to ensure completeness and integrity of audit data for election software. These operating systems are capable of executing multiple application programs simultaneously. These systems include both servers and workstations, including the many varieties of UNIX and Linux, and those offered by Microsoft and Apple. Election software running on these systems is vulnerable to unintended effects from other user sessions, applications, and utilities executing on the same platform at the same time as the election software.

“Simultaneous processes” of concern include: unauthorized network connections, unplanned user logins, and unintended execution or termination of operating system processes. An unauthorized network connection or unplanned user login can host unintended processes and user actions, such as the termination of operating system audit, the termination of election software processes, or the deletion of election software audit and logging data. The execution of an operating system process could be a full system scan at a time when that process would adversely affect the election software processes. Operating system processes improperly terminated could be system audit or malicious code detection.

To counter these vulnerabilities, three operating system protections are required on all such systems on which election software is hosted. First, authentication shall be configured on the local terminal (display screen and keyboard) and on all external connection devices (“network cards” and “ports”). This ensures that only authorized and identified users affect the system while election software is running.

Second, operating system audit shall be enabled for all session openings and closings, for all connection openings and closings, for all process executions and terminations, and for the alteration or deletion of any memory or file object. This ensures the accuracy and completeness of election data stored on the system. It also ensures the existence of an audit record of any person or process altering or deleting system data or election data.

Third, the system shall be configured to execute only intended and necessary processes during the execution of election software. The system shall also be configured to halt election software processes upon the termination of any critical system process (such as system audit) during the execution of election software.

2.1.6 Election Management System

The Election Management System (EMS) is used to prepare ballots and programs for use in casting and counting votes, and to consolidate, report, and display election results. An EMS shall generate and maintain a database, or one or more interactive databases, that enables election officials or their designees to perform the following functions:

- Define political subdivision boundaries and multiple election districts as indicated in the system documentation
- Identify contests, candidates, and issues
- Define ballot formats and appropriate voting options
- Generate ballots and election-specific programs for voting equipment
- Install ballots and election-specific programs
- Test that ballots and programs have been properly prepared and installed
- Accumulate vote totals at multiple reporting levels as indicated in the system documentation
- Generate the post-voting reports required by Subsection 2.4
- Process and produce audit reports of the data as indicated in Subsection 5.5

2.1.7 Vote Tabulating Program

Each voting system shall have a vote tabulation program that will meet specific functional requirements.

2.1.7.1 Functions

The vote tabulating program software resident in each voting machine, vote count server, or other devices shall include all software modules required to:

- a. Monitor system status and generate machine-level audit reports

- b. Accommodate device control functions performed by polling place officials and maintenance personnel
- c. Register and accumulate votes
- d. Accommodate variations in ballot counting logic

2.1.7.2 Voting Variations

There are significant variations among state election laws with respect to permissible ballot contents, voting options, and the associated ballot counting logic. The Technical Data Package accompanying the system shall specifically identify which of the following items *can* and *cannot* be supported by the voting system, as well as *how* the voting system can implement the items supported:

- Closed primaries
- Open primaries
- Partisan offices
- Non-partisan offices
- Write-in voting
- Primary presidential delegation nominations
- Ballot rotation
- Straight party voting
- Cross-party endorsement
- Split precincts
- Vote for N of M
- Recall issues, with options
- Cumulative voting
- Ranked order voting
- Provisional or challenged ballots

2.1.8 Ballot Counter

For all voting systems, each piece of voting equipment that tabulates ballots shall provide a counter that:

- a. Can be set to zero before any ballots are submitted for tally
- b. Records the number of ballots cast during a particular test cycle or election
- c. Increases the count only by the input of a ballot
- d. Prevents or disables the resetting of the counter by any person other than authorized persons at authorized points

- e. Is visible to designated election officials

2.1.9 Telecommunications

For all voting systems that use telecommunications for the transmission of data during pre-voting, voting or post-voting activities, capabilities shall be provided that ensure data are transmitted with no alteration or unauthorized disclosure during transmission. Such transmissions shall not violate the privacy, secrecy, and integrity demands of the *Guidelines*. Section 6 describes telecommunications standards that apply to, at a minimum, the following types of data transmissions:

Voter Authentication: Coded information that confirms the identity of a voter for security purposes for a system that transmit votes individually over a public network

Ballot Definition: Information that describes to voting equipment the content and appearance of the ballots to be used in an election

Vote Transmission to Central Site: For voting systems that transmit votes individually over a public network, the transmission of a single vote to the county (or contractor) for consolidation with other county vote data

Vote Count: Information representing the tabulation of votes at any one of several levels: polling place, precinct, or central count

List of Voters: A listing of the individual voters who have cast ballots in a specific election

2.1.10 Data Retention

United States Code Title 42, Sections 1974 through 1974e state that election administrators shall preserve for 22 months “all records and paper that came into (their) possession relating to an application, registration, payment of poll tax, or other act requisite to voting.” This retention requirement applies to systems that will be used at anytime for voting of candidates for federal offices (e.g., Member of Congress, United States Senator, and/or Presidential Elector). Therefore, all voting systems shall provide for maintaining the integrity of voting and audit data during an election and for a period of at least 22 months thereafter.

Because the purpose of this law is to assist the federal government in discharging its law enforcement responsibilities in connection with civil rights and elections crimes, its scope must be interpreted in keeping with that objective. The appropriate state or local authority must preserve all records that may be relevant to the detection and prosecution of federal civil rights or election crimes for the 22-month federal retention period, if the records were generated in connection with an election that was held in whole or in part to select federal candidates. It is important to note that Section 1974 does not require that election officials generate any specific type or classification of election record. However, if a record is

generated, Section 1974 comes into force and the appropriate authority must retain the records for 22 months.

For 22-month document retention, the general rule is that all printed copy records produced by the election database and ballot processing systems shall be so labeled and archived. Regardless of system type, all audit trail information spelled out in Subsection 5.5 shall be retained in its original format, whether that be real-time logs generated by the system, or manual logs maintained by election personnel. The election audit trail includes not only in-process logs of election-night and subsequent processing of absentee or provisional ballots, but also time logs of baseline ballot definition formats, and system readiness and testing results.

In many voting systems, the source of election-specific data (and ballot formats) is a database or file. In precinct count voting systems, this data is used to program each machine, establish ballot layout, and generate tallying files. It is not necessary to retain this information on electronic media if there is an official, authenticated printed copy of all final database information. However, it is recommended that the state or local jurisdiction also retain electronic records of the aggregate data for each voting machine so that reconstruction of an election is possible without data re-entry. The same requirement and recommendation applies to vote results generated by each precinct count voting machine.

2.2 Pre-voting Capabilities

This subsection defines capabilities required to support functions performed prior to the opening of polls. All voting systems shall provide capabilities to support:

- Ballot preparation
- Election programming
- Ballot and program installation and control
- Readiness testing
- Verification at the polling place
- Verification at the central counting place

The standards also include requirements to ensure compatible interfaces with the ballot definition process and the reporting of election results.

2.2.1 Ballot Preparation

Ballot preparation is the process of using election databases to define the specific contests, questions, and related instructions to be contained in ballots and to produce all permissible ballot layouts. Ballot preparation requirements include:

- General capabilities
- Ballot formatting
- Ballot production

2.2.1.1 General Capabilities

All systems shall provide the general capabilities for ballot preparation. All systems shall be capable of:

- a. Enabling the automatic formatting of ballots in accordance with the requirements for offices, candidates, and measures qualified to be placed on the ballot for each political subdivision and election district
- b. Collecting and maintaining the following data
 - i. Offices and their associated labels and instructions
 - ii. Candidate names and their associated labels
 - iii. Issues or measures and their associated text
- c. Supporting the maximum number of potentially active voting positions as indicated in the system documentation
- d. For a primary election, generating ballots that segregate the choices in partisan contests by party affiliation
- e. Generating ballots that contain identifying codes or marks uniquely associated with each format
- f. Ensuring that vote response fields, selection buttons, or switches properly align with the specific candidate names and/or issues printed on the ballot display, ballot card or sheet, or separate ballot pages

Paper-based voting systems shall also meet the following requirements applicable to the technology used:

- g. Enable voters to make selections by making a mark in areas designated for this purpose upon each ballot sheet
- h. For marksense systems, ensure that the timing marks align properly with the vote response fields

2.2.1.2 Ballot Formatting

Ballot formatting is the process by which election officials or their designees use election databases and voting system software to define the specific contests and related instructions contained on the ballot and present them in a layout permitted by state law. All voting systems shall provide a capability for:

- a. Creation of newly defined elections

- b. Rapid and error-free definition of elections and their associated ballot layouts
- c. Uniform allocation of space and fonts used for each office, candidate, and contest such that the voter perceives no active voting position to be preferred to any other
- d. Simultaneous display of the maximum number of choices for a single contest as indicated by the vendor in the system documentation
- e. Retention of previously defined formats for an election
- f. Prevention of unauthorized modification of any ballot formats
- g. Modification by authorized persons of a previously defined ballot format for use in a subsequent election

2.2.1.3 Ballot Production

Ballot production is the process of converting ballot formats to a media ready for use in the physical ballot production or electronic presentation.

The voting system shall provide a means of printing or otherwise generating a ballot display that can be installed in all voting equipment for which it is intended. All voting systems shall provide the capabilities below.

- a. The electronic display or printed document on which the user views the ballot is capable of rendering an image of the ballot in any of the languages required by the Voting Rights Act of 1965, as amended.
- b. The electronic display or printed document on which the user views the ballot does not show any advertising or commercial logos of any kind, whether public service, commercial, or political, unless specifically provided for in state law. Electronic displays shall not provide connection to such material through hyperlink.
- c. The ballot conforms to vendor specifications for type of paper stock, weight, size, shape, size and location of mark field used to record votes, folding, bleed-through, and ink for printing if paper ballot documents or paper displays are part of the system.

Vendor documentation for marksense systems shall include specifications for ballot materials to ensure that vote selections are read from only a single ballot at a time, without detection of marks from multiple ballots concurrently (e.g., reading of bleed-through from other ballots).

2.2.2 Election Programming

Election programming is the process by which election officials or their designees use election databases and vendor system software to logically define the voter choices associated with the contents of the ballots. All systems shall provide for the:

- a. Logical definition of the ballot, including the definition of the number of allowable choices for each office and contest
- b. Logical definition of political and administrative subdivisions, where the list of candidates or contests varies between polling places
- c. Exclusion of any contest on the ballot in which the voter is prohibited from casting a ballot because of place of residence, or other such administrative or geographical criteria
- d. Ability to select from a range of voting options to conform to the laws of the jurisdiction in which the system will be used
- e. Generation of all required master and distributed copies of the voting program, in conformance with the definition of the ballots for each voting device and polling place, and for each tabulating device

2.2.3 Ballot and Program Installation and Control

All systems shall provide a means of installing ballots and programs on each piece of polling place or central count equipment in accordance with the ballot requirements of the election and the requirements of the jurisdiction in which the equipment will be used. All systems shall include the following at the time of ballot and program installation:

- a. A detailed work plan or other documentation providing a schedule and steps for the software and ballot installation, which includes a table outlining the key dates, events and deliverables
- b. A capability for automatically verifying that the software has been properly selected and installed in the equipment or in programmable memory devices, and for indicating errors
- c. A capability for automatically validating that software correctly matches the ballot formats that it is intended to process, for detecting errors, and for immediately notifying an election official of detected errors

2.2.4 Readiness Testing

Election personnel conduct voting equipment and voting system readiness tests prior to the start of an election to ensure that the voting system functions properly, to confirm that voting equipment has been properly integrated, and to obtain equipment status reports. All voting systems shall provide the capabilities to:

- a. Verify that voting equipment and precinct count equipment is properly prepared for an election, and collect data that verifies equipment readiness

- b. Obtain status and data reports from each set of equipment
- c. Verify the correct installation and interface of all voting equipment
- d. Verify that hardware and software function correctly
- e. Generate consolidated data reports at the polling place and higher jurisdictional levels
- f. Segregate test data from actual voting data, either procedurally or by hardware/software features

Resident test software, external devices, and special purpose test software connected to or installed in voting equipment to simulate operator and voter functions may be used for these tests provided that the following standards are met:

- g. These elements shall be capable of being tested separately, and shall be proven to be reliable verification tools prior to their use
- h. These elements shall be incapable of altering or introducing any residual effect on the intended operation of the voting device during any succeeding test and operational phase

Paper-based systems shall:

- i. Support conversion testing that uses all potential ballot positions as active positions
- j. Support conversion testing of ballots with active position density for systems without pre-designated ballot positions

2.2.5 Verification at the Polling Place

Election officials perform verification at the polling place to ensure that all voting systems and voting equipment function properly before and during an election. All voting systems shall provide a formal record of the following, in any media, upon verification of the authenticity of the command source:

- a. The election's identification data
- b. The identification of all equipment units
- c. The identification of the polling place
- d. The identification of all ballot formats
- e. The contents of each active candidate register by office and of each active measure register at all storage locations (showing that they contain only zeros)
- f. A list of all ballot fields that can be used to invoke special voting options

- g. Other information needed to confirm the readiness of the equipment, and to accommodate administrative reporting requirements

To prepare voting devices to accept voted ballots, all voting systems shall provide the capability to test each device prior to opening to verify that each is operating correctly. At a minimum, the tests shall include:

- h. Confirmation that there are no hardware or software failures
- i. Confirmation that the device is ready to be activated for accepting votes

If a precinct count system includes equipment for the consolidation of polling place data at one or more central counting locations, it shall have means to verify the correct extraction of voting data from transportable memory devices, or to verify the transmission of secure data over secure communication links.

2.2.6 Verification at the Central Location

Election officials perform verification at the central location to ensure that vote counting and vote consolidation equipment and software function properly before and after an election. Upon verification of the authenticity of the command source, any system used in a central count environment shall provide a printed record of the following:

- a. The election's identification data
- b. The contents of each active candidate register by office and of each active measure register at all storage locations (showing that they contain all zeros)
- c. Other information needed to ensure the readiness of the equipment and to accommodate administrative reporting requirements

2.3 Voting Capabilities

All voting systems shall support:

- Opening the polls
- Casting a ballot

Additionally, all DRE systems shall support:

- Activating the ballot
- Augmenting the election counter
- Augmenting the life-cycle counter

2.3.1 Opening the Polls

The capabilities required for opening the polls are specific to individual voting system technologies. At a minimum, the systems shall provide the functional capabilities indicated below.

2.3.1.1 Precinct Count Systems

To allow voting devices to be activated for voting, all precinct count systems shall provide:

- a. An internal test or diagnostic capability to verify that all of the polling place tests specified in Subsection 2.2.5 have been successfully completed
- b. Automatic disabling of any device that has not been tested until it has been tested

2.3.1.2 Paper-based System Requirements

To facilitate opening the polls, all paper-based systems shall include:

- a. A means of verifying that ballot marking devices are properly prepared and ready to use
- b. A voting booth or similar facility, in which the voter may mark the ballot in privacy
- c. Secure receptacles for holding voted ballots

In addition to the above requirements, all paper-based precinct count equipment shall include a means of:

- d. Activating the ballot counting device
- e. Verifying that the device has been correctly activated and is functioning properly
- f. Identifying device failure and corrective action needed

2.3.1.3 DRE System Requirements

To facilitate opening the polls, all DRE systems shall include:

- a. A security seal, a password, or a data code recognition capability to prevent the inadvertent or unauthorized actuation of the poll-opening function
- b. A means of enforcing the execution of steps in the proper sequence if more than one step is required

- c. A means of verifying the system has been activated correctly
- d. A means of identifying system failure and any corrective action needed

2.3.2 Activating the Ballot (DRE Systems)

To activate the ballot, all DRE systems shall:

- a. Enable election officials to control the content of the ballot presented to the voter, whether presented in printed form or electronic display, such that each voter is permitted to record votes only in contests in which that voter is authorized to vote
- b. Allow each eligible voter to cast a ballot
- c. Prevent a voter from voting on a ballot to which he or she is not entitled
- d. Prevent a voter from casting more than one ballot in the same election
- e. Activate the casting of a ballot in a general election
- f. Enable the selection of the ballot that is appropriate to the party affiliation declared by the voter in a primary election
- g. Activate all portions of the ballot upon which the voter is entitled to vote
- h. Disable all portions of the ballot upon which the voter is not entitled to vote

2.3.3 Casting a Ballot

Some required capabilities for casting a ballot are common to all systems. Others are specific to individual voting technologies or intended use. Systems must provide additional functional capabilities that enable accessibility to disabled voters as defined in Subsection 3.2.

2.3.3.1 Common Requirements

To facilitate casting a ballot, all systems shall:

- a. Provide text that is at least 3 millimeters high and provide the capability to adjust or magnify the text to an apparent size of 6.3 millimeters
- b. Protect the secrecy of the vote such that the system cannot reveal any information about how a particular voter voted, except as otherwise required by individual state law

- c. Record the selection and non-selection of individual vote choices for each contest and ballot measure
- d. Record the voter's selection of candidates whose names do not appear on the ballot, if permitted under state law, and record as many write-in votes as the number of candidates the voter is allowed to select
- e. In the event of a failure of the main power supply external to the voting system, provide the capability for any voter who is voting at the time to complete casting a ballot, allow for the successful shutdown of the voting system without loss or degradation of the voting and audit data, and allow voters to resume voting once the voting system has reverted to back-up power
- f. Provide the capability for voters to continue casting ballots in the event of a failure of a telecommunications connection within the polling place or between the polling place and any other location

2.3.3.2 Paper-based System Requirements

All paper-based systems shall:

- a. Allow the voter to easily identify the voting field that is associated with each candidate or ballot measure response
- b. Allow the voter to mark the ballot to register a vote
- c. Allow either the voter or the appropriate election official to place the voted ballot into the ballot counting device (for precinct count systems) or into a secure receptacle (for central count systems)
- d. Protect the secrecy of the vote throughout the process

In addition to the above requirements, all paper-based precinct count systems shall:

- e. Provide feedback to the voter that identifies specific contests for which he or she has made no selection or fewer than the allowable number of selections (e.g., undervotes)
- f. Notify the voter if he or she has made more than the allowable number of selections for any contest (e.g., overvotes)
- g. Notify the voter before the ballot is cast and counted of the effect of making more than the allowable number of selections for a contest
- h. Provide the voter opportunity to correct the ballot for either an undervote or overvote before the ballot is cast and counted

2.3.3.3 DRE System Requirements

In addition to the above common requirements, DRE systems shall:

- a. Prohibit the voter from accessing or viewing any information on the display screen that has not been authorized by election officials and preprogrammed into the voting system (i.e., no potential for display of external information or linking to other information sources)
- b. Enable the voter to easily identify the selection button or switch, or the active area of the ballot display, that is associated with each candidate or ballot measure response
- c. Allow the voter to select his or her preferences on the ballot in any legal number and combination
- d. Indicate that a selection has been made or canceled
- e. Indicate to the voter when no selection, or an insufficient number of selections, has been made for a contest (e.g., undervotes)
- f. Notify the voter if he or she has made more than the allowable number of selections for any contest (e.g., overvotes)
- g. Notify the voter before the ballot is cast and counted of the effect of making more than the allowable number of selections for a contest
- h. Provide the voter opportunity to correct the ballot for either an undervote or overvote before the ballot is cast and counted
- i. Notify the voter when the selection of candidates and measures is completed
- j. Allow the voter, before the ballot is cast, to review his or her choices and, if the voter desires, to delete or change his or her choices before the ballot is cast
- k. For electronic image displays, prompt the voter to confirm the voter's choices before casting his or her ballot, signifying to the voter that casting the ballot is irrevocable and directing the voter to confirm the voter's intention to cast the ballot
- l. Notify the voter after the vote has been stored successfully that the ballot has been cast
- m. Notify the voter that the ballot has not been cast successfully if it is not stored successfully, including storage of the ballot image, and provide clear instruction as to the steps the voter should take to cast his or her ballot should this event occur
- n. Provide sufficient computational performance to provide responses back to each voter entry in no more than three seconds

- o. Ensure that the votes stored accurately represent the actual votes cast
- p. Prevent modification of the voter's vote after the ballot is cast
- q. Provide a capability to retrieve ballot images in a form readable by humans [in accordance with the requirements of Subsections 2.1.2 (f) and 2.1.4 (k) and (l)]
- r. Increment the proper ballot position registers or counters
- s. Protect the secrecy of the vote throughout the voting process
- t. Prohibit access to voted ballots until after the close of polls
- u. Provide the ability for election officials to submit test ballots for use in verifying the end-to-end integrity of the voting system
- v. Isolate test ballots such that they are accounted for accurately in vote counts and are not reflected in official vote counts for specific candidates or measures

2.4 Post-Voting Capabilities

All voting systems shall provide capabilities to accumulate and report results for the jurisdiction and to generate audit trails. In addition, precinct count voting systems must provide a means to close the polls including generating appropriate reports. If the system provides the capability to broadcast results, additional standards apply.

2.4.1 Closing the Polls

These requirements for closing the polls and locking voting systems against future voting are specific to precinct count systems. The voting system shall provide the means for:

- a. Preventing the further casting of ballots once the polls have closed
- b. Providing an internal test that verifies that the prescribed closing procedure has been followed, and that the device status is normal
- c. Incorporating a visible indication of system status
- d. Producing a diagnostic test record that verifies the sequence of events, and indicates that the extraction of voting data has been activated
- e. Precluding the unauthorized reopening of the polls once the poll closing has been completed for that election

2.4.2 Consolidating Vote Data

All systems shall provide a means to consolidate vote data from all polling places, and optionally from other sources such as absentee ballots, provisional ballots, and voted ballots requiring human review (e.g., write-in votes).

2.4.3 Producing Reports

All systems shall be able to create reports summarizing the vote data on multiple levels.

All systems shall provide capabilities to:

- a. Support geographic reporting, which requires the reporting of all results for each contest at the precinct level and additional jurisdictional levels
- b. Produce a printed report of the number of ballots counted by each tabulator
- c. Produce a printed report for each tabulator of the results of each contest that includes the votes cast for each selection, the count of undervotes, and the count of overvotes
- d. Produce a consolidated printed report of the results for each contest of all votes cast (including the count of ballots from other sources supported by the system as specified by the vendor) that includes the votes cast for each selection, the count of undervotes, and the count of overvotes
- e. Be capable of producing a consolidated printed report of the combination of overvotes for any contest that is selected by an authorized official (e.g., the number of overvotes in a given contest combining candidate A and candidate B, combining candidate A and candidate C, etc.)
- f. Produce all system audit information required in Subsection 5.4 in the form of printed reports, or in electronic memory for printing centrally
- g. Prevent data from being altered or destroyed by report generation, or by the transmission of results over telecommunications lines

In addition, all precinct count voting systems shall:

- h. Prevent the printing of reports and the unauthorized extraction of data prior to the official close of the polls
- i. Provide a means to extract information from a transportable programmable memory device or data storage medium for vote consolidation
- j. Consolidate the data contained in each unit into a single report for the polling place when more than one voting machine or precinct tabulator is used

- k. Prevent data in transportable memory from being altered or destroyed by report generation, or by the transmission of official results over telecommunications lines

2.4.4 Broadcasting Results

Some voting systems offer the capability to make unofficial results available to external organizations such as the news media, political party officials, and others. Although this capability is not required, systems that make unofficial results available shall:

- a. Provide only aggregated results, and not data from individual ballots
- b. Provide no access path from unofficial electronic reports or files to the storage devices for official data
- c. Clearly indicate on each report or file that the results it contains are unofficial

2.5 Maintenance, Transportation, and Storage

All systems shall be designed and manufactured to facilitate preventive and corrective maintenance, conforming to the hardware standards described in Subsection 4.1. All vote casting and tally equipment designated for storage between elections shall:

- a. Function without degradation in capabilities after transit to and from the place of use, as demonstrated by meeting the performance standards described in Subsection 4.1
- b. Function without degradation in capabilities after storage between elections, as demonstrated by meeting the performance standards described in Subsection 4.1

[Intentionally left blank]

3 Usability and Accessibility Requirements

Table of Contents

3	Usability and Accessibility Requirements	45
3.1	Usability Requirements	46
3.1.1	Usability Testing	48
3.1.2	Functional Capabilities	48
3.1.3	Alternative Languages	49
3.1.4	Cognitive Issues	49
3.1.5	Perceptual Issues	51
3.1.6	Interaction Issues	52
3.1.7	Privacy	53
3.1.7.1	Privacy at the Polls	53
3.1.7.2	No Recording of Alternate Format Usage	53
3.2	Accessibility Requirements	53
3.2.1	General	54
3.2.2	Vision	55
3.2.2.1	Partial Vision	55
3.2.2.2	Blindness	56
3.2.3	Dexterity	59
3.2.4	Mobility	60
3.2.5	Hearing	64
3.2.6	Speech	64
3.2.7	English Proficiency	64
3.2.8	Cognition	64

[Intentionally left blank]

3 Usability and Accessibility Requirements

The importance of usability and accessibility in the design of voting systems has become increasingly apparent. It is not sufficient that the internal operation of these systems be correct; in addition, voters and poll workers must be able to use them effectively. There are some particular considerations for the design of usable and accessible voting systems:

- The voting task itself can be fairly complex; the voter may have to navigate an electronic ballot, choose multiple candidates in a single contest, or decide on abstrusely worded referenda
- Voting is performed infrequently, so there is limited opportunity for voters and poll workers to gain familiarity with the process
- Jurisdictions may change voting equipment, thus obviating whatever familiarity the voter might have acquired
- Usability and accessibility requirements include a broad range of factors, including physical abilities, language skills, and technology experience

The challenge, then, is to provide a voting system that voters can use comfortably, efficiently, and with confidence that they have cast their votes correctly. The requirements within this section are intended to serve that goal. Three broad principles motivate this section:

1. All eligible voters shall have access to the voting process without discrimination.

The voting process shall be accessible to individuals with disabilities. The voting process includes access to the polling place, instructions on how to vote, initiating the voting session, making ballot selections, review of the ballot, final submission of the ballot, and getting help when needed.

2. Each cast ballot shall accurately capture the selections made by the voter.

The ballot shall be presented to the voter in a manner that is clear and usable. Voters should encounter no difficulty or confusion regarding the process for recording their selections.

3. The voting process shall preserve the secrecy of the ballot.

The voting process shall preclude anyone else from determining the content of a voter's ballot, without the voter's cooperation. If such a determination is made against the wishes of the voter, then his or her privacy has been violated.

All the requirements in this section have the purpose of improving the quality of interaction between voters and voting systems.

- Requirements for general usability apply to all voting systems. Requirements for any alternative languages required by state or federal law are included under this heading.

- Requirements to assist voters with physical, sensory, or cognitive disabilities apply, as a minimum, to the accessible voting stations required by HAVA Section 301 (a)(3)(B). They may also assist those not usually described as having a disability, e.g., voters with poor eyesight or limited dexterity.

Several uncommon terms are used in this section. For the convenience of the reader, they are defined below, in addition to being included in the Glossary. Other terms frequently used here and throughout this document are defined in the Glossary. Note in particular the distinctions between these terms: voting system, voting equipment, voting machine and voting station.

- Common Industry Format (CIF) - the format to be used for usability testing reporting, described in ANSI/INCITS 354-2001 "Common Industry Format (CIF) for Usability Test Reports"
- Accessible Voting Station – the voting station equipped for individuals with disabilities referred to in HAVA 301 (a)(3)(B).
- Audio-Tactile Interface - a voter interface designed not to require visual reading of a ballot. Audio is used to convey information to the voter and sensitive tactile controls allow the voter to convey information to the voting system.

3.1 Usability Requirements

The voting process shall provide a high level of usability for voters. Accordingly, voters shall be able to negotiate the process effectively, efficiently, and comfortably. The mandatory voting system standards mandated in HAVA Section 301 relate to the interaction between the voter and the voting system:

a. Requirements.--Each voting system used in an election for federal office shall meet the following requirements:

1. In general.--

A. Except as provided in subparagraph (B), the voting system (including any lever voting system, optical scanning voting system, or direct recording electronic system) shall--

i. Permit the voter to verify (in a private and independent manner) the votes selected by the voter on the ballot before the ballot is cast and counted;

ii. Provide the voter with the opportunity (in a private and independent manner) to change the ballot or correct any error before the ballot is cast and counted (including the opportunity to correct the error through the issuance of a replacement ballot if the voter was otherwise unable to change the ballot or correct any error); and

iii. If the voter selects votes for more than one candidate for a single office--

I. Notify the voter that the voter has selected more than one candidate for a single office on the ballot;

II. Notify the voter before the ballot is cast and counted of the effect of casting multiple votes for the office; and

III. Provide the voter with the opportunity to correct the ballot before the ballot is cast and counted.

B. A state or jurisdiction that uses a paper ballot voting system, a punch card voting system, or a central count voting system (including mail-in absentee ballots and mail-in ballots), may meet the requirements of subparagraph (A)(iii) by—

i. Establishing a voter education program specific to that voting system that notifies each voter of the effect of casting multiple votes for an office; and

ii. Providing the voter with instructions on how to correct the ballot before it is cast and counted (including instructions on how to correct the error through the issuance of a replacement ballot if the voter was otherwise unable to change the ballot or correct any error).

C. The voting system shall ensure that any notification required under this paragraph preserves the privacy of the voter and the confidentiality of the ballot.

Usability is defined generally as a measure of the effectiveness, efficiency, and satisfaction achieved by a specified set of users with a given product in the performance of specified tasks. In the context of voting, the primary user is the voter, the product is the voting system, and the task is the correct recording of the voter ballot selections. Additional requirements for task performance are independence and privacy: the voter should normally be able to complete the voting task without assistance from others, and the voter selections should be private. Lack of independence or privacy may adversely affect effectiveness (e.g., by possibly inhibiting the voter's free choice) and efficiency (e.g., by slowing down the process).

Among the basic metrics for usability are:

- low error rate for marking the ballot (the voter selection is correctly conveyed to and represented within the voting system)
- efficient operation (time required to vote is not excessive)
- satisfaction (voter experience is safe, comfortable, free of stress, and instills confidence)

It is the intention of the EAC that in future revisions to the *Guidelines*, usability will be addressed by high-level performance-based requirements. That is, the requirements will directly address metrics for effectiveness (e.g., correct capture of voter selections), efficiency (e.g., time taken to vote), and satisfaction. Until the supporting research is completed, however, the contents of this subsection are limited to a basic set of widely accepted design requirements and lower-level performance requirements. The reasons for this approach are:

- These are to serve as interim requirements, pending the issuance of high-level performance requirements

- The actual benefit of numerous detailed design guidelines is difficult to prove or measure
- The technical complexity and costs of a large set of detailed requirements may not be justified
- Guidelines that are difficult to test because of insufficient specificity have been omitted

While the scope of usability applies to the entire voting process, the emphasis in these requirements is on the voter interface with the voting machine, which is assumed to be a visual-tactile interface.

The outline for this subsection is:

- 3.1.1 Usability Testing
- 3.1.2 Functional Capabilities
- 3.1.3 Alternative Languages
- 3.1.4 Cognitive Issues
- 3.1.5 Perceptual Issues
- 3.1.6 Interaction Issues
- 3.1.7 Privacy

3.1.1 Usability Testing

The vendor shall conduct summative usability tests on the voting system using individuals representative of the general population. The vendor shall document the testing performed and report the test results using the Common Industry Format. This documentation shall be included in the Technical Data Package submitted to the EAC for national certification.

Discussion: Voting system developers are required to conduct realistic usability tests on the final product. For the present, vendors can define their own testing protocols. Future revisions to the *Guidelines* will include requirements for usability testing that will provide specific performance benchmarks.

3.1.2 Functional Capabilities

The voting process shall provide certain functional capabilities to support voter usability.

- a. The voting system shall provide feedback to the voter that identifies specific contests or ballot issues for which he or she has made no selection or fewer than the allowable number of selections (e.g., undervotes)
- b. The voting system shall notify the voter if he or she has made more than the allowable number of selections for any contest (e.g., overvotes)
- c. The voting system shall notify the voter before the ballot is cast and counted of the effect of making more than the allowable number of selections for a contest

- d. The voting system shall provide the voter the opportunity to correct the ballot for either an undervote or overvote before the ballot is cast and counted
- e. The voting system shall allow the voter, at his or her choice, to submit an undervoted ballot without correction
- f. DRE voting machines shall allow the voter to change a vote within a contest before advancing to the next contest.

Discussion: The point here is that voters using a DRE should not have to wait for the final ballot review screen in order to change a vote.

- g. DRE voting machines should provide navigation controls that allow the voter to advance to the next contest or go back to the previous contest before completing a vote on the contest currently being presented (whether visually or aurally).

Discussion: For example, the voter should not be forced to proceed sequentially through all the contests before going back to check his or her selection for a previous contest.

3.1.3 Alternative Languages

The voting equipment shall be capable of presenting the ballot, ballot selections, review screens and instructions in any language required by state or federal law.

Discussion: HAVA Section 301 (a)(4) states that the voting system shall provide alternative language accessibility pursuant to the requirements of section 203 of the Voting Rights Act of 1965 (42 U.S.C. 1973aa-1a). Ideally every voter would be able to vote independently and privately, regardless of language. As a practical matter, alternative language access is mandated under the Voting Rights Act of 1975, subject to certain thresholds, e.g., if the language group exceeds 5% of the voting age population. The audio interface provided for blind voters may also assist voters who speak English, but who are unable to read it (See Subsection 3.2.2.2).

3.1.4 Cognitive Issues

The voting process shall be designed to minimize cognitive difficulties for the voter.

- a. Consistent with election law, the voting system should support a process that does not introduce any bias for or against any of the selections to be made by the voter. In both visual and aural formats, contest choices shall be presented in an equivalent manner.

Discussion: Certain differences in presentation are mandated by state law, such as the order in which candidates are listed and provisions for voting for write-in

candidates. But comparable characteristics such as font size or voice volume and speed must be the same for all choices.

- b. The voting machine or related materials shall provide clear instructions and assistance to allow voters to successfully execute and cast their ballots independently.

Discussion: Voters should not routinely need to ask for human assistance.

- i. Voting machines or related materials shall provide a means for the voter to get help at any time during the voting session.

Discussion: The voter should always be able to get help if needed. DRE voting machines may provide this with a distinctive “help” button. Any type of voting equipment may provide written instructions that are separate from the ballot.

- ii. The voting machine shall provide instructions for all its valid operations.

Discussion: If an operation is available to the voter, it must be documented. Examples include how to change a vote, how to navigate among contests, how to cast a straight party vote, and how to cast a write-in vote.

- c. The voting system shall provide the capability to design a ballot for maximum clarity and comprehension.

- i. The voting equipment should not visually present a single contest spread over two pages or two columns.

Discussion: Such a visual separation poses the risk that the voter may perceive one contest as two. If a contest has a large number of candidates, it may be infeasible to observe this guideline.

- ii. The ballot shall clearly indicate the maximum number of candidates for which one can vote within a single contest.

- iii. There shall be a consistent relationship between the name of a candidate and the mechanism used to vote for that candidate.

Discussion: For example, if the response field where voters indicate their selections is located to the left of a candidate’s name, then each response field shall be located to the left of the associated candidates’ names.

- d. Warnings and alerts issued by the voting system should clearly state the nature of the problem and the set of responses available to the voter. The warning should clearly state whether the voter has performed or attempted an invalid operation or whether the voting equipment itself has malfunctioned in some way.

Discussion: In case of an equipment failure, the only action available to the voter might be to get assistance from a poll worker.

- e. The use of color by the voting system should agree with common conventions: (a) green, blue or white is used for general information or as a normal status indicator; (b) amber or yellow is used to indicate warnings or a marginal status; (c) red is used to indicate error conditions or a problem requiring immediate attention.

3.1.5 Perceptual Issues

The voting process shall be designed to minimize perceptual difficulties for the voter.

- a. No voting machine display screen shall flicker with a frequency between 2 Hz and 55 Hz.

Discussion: Aside from usability concerns, this requirement protects voters with epilepsy.

- b. Any aspect of the voting machine that is adjustable by the voter or poll worker, including font size, color, contrast, and audio volume, shall automatically reset to a standard default value upon completion of that voter's session.

Discussion: The voting machine must present the same initial appearance to every voter.

- c. If any aspect of a voting machine is adjustable by the voter or poll worker, there shall be a mechanism to reset all such aspects to their default values.

Discussion: The purpose is to allow a voter who has adjusted the machine into an undesirable state to reset all the aspects to begin again.

- d. All electronic voting machines shall provide a minimum font size of 3.0 mm (measured as the height of a capital letter) for all text.

- e. All voting machines using paper ballots should make provisions for voters with poor reading vision.

Discussion: Possible solutions include: (a) providing paper ballots in at least two font sizes, 3.0-4.0mm and 6.3-9.0mm and (b) providing a magnifying device.

- f. The default color coding shall maximize correct perception by voters with color blindness.

Discussion: There are many types of color blindness and no color coding can, by itself, guarantee correct perception for everyone. However, designers should take into account such factors as: red-green color blindness is the most common form; high luminosity contrast will help colorblind voters to recognize visual features; and color-coded graphics can also use shape to improve the ability to distinguish certain features.

- g. Color coding shall not be used as the sole means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.

Discussion: While color can be used for emphasis, some other non-color mode must also be used to convey the information, such as a shape or text style. For example, red can be enclosed in an octagon shape.

- h. All text intended for the voter should be presented in a sans serif font.

Discussion: Experimentation has shown that users prefer such a font and the legibility of serif and sans serif fonts is equivalent.

- i. The minimum figure-to-ground ambient contrast ratio for all text and informational graphics (including icons) intended for the voter shall be 3:1.

3.1.6 Interaction Issues

The voting process shall be designed to minimize interaction difficulties for the voter.

- a. Voting machines with electronic image displays shall not require page scrolling by the voter.

Discussion: This is not an intuitive operation for those unfamiliar with the use of computers. Even those experienced with computers often do not notice a scroll bar and miss information at the bottom of the "page." Voting systems may require voters to move to the next or previous "page."

- b. The voting machine shall provide unambiguous feedback regarding the voter's selection, such as displaying a checkmark beside the selected option or conspicuously changing its appearance.

- c. If the voting machine requires a response by a voter within a specific period of time, it shall issue an alert at least 20 seconds before this time period has expired and provide a means by which the voter may receive additional time.

- d. Input mechanisms shall be designed to minimize accidental activation.

- i. On touch screens, the sensitive touch areas shall have a minimum height of 0.5 inches and minimum width of 0.7 inches. The vertical distance between the centers of adjacent areas shall be at least 0.6 inches, and the horizontal distance at least 0.8 inches.

- ii. No key or control on a voting machine shall have a repetitive effect as a result of being held in its active position.

Discussion: This is to preclude accidental activation. For instance, if a voter is typing in the name of a write-in candidate, depressing and holding the "e" key results in only a single "e" added to the name.

3.1.7 Privacy

The voting process shall preclude anyone else from determining the content of a voter's ballot, without the voter's cooperation.

Discussion: Privacy ensures that the voter can make selections based solely on his or her own preferences without intimidation or inhibition. Among other practices, this forbids the issuance of a receipt to the voter that would provide proof of how he or she voted.

3.1.7.1 Privacy at the Polls

When deployed according to the installation instructions provided by the vendor, the voting station shall prevent others from observing the contents of a voter's ballot.

- a. The ballot and any input controls shall be visible only to the voter during the voting session and ballot submission.
- b. The audio interface shall be audible only to the voter.

Discussion: Voters who are hard of hearing but need to use an audio interface may also need to increase the volume of the audio. Such situations require headphones with low sound leakage.

- c. As mandated by HAVA 301 (a)(1)(C), the voting system shall notify the voter of an attempted overvote in a way that preserves the privacy of the voter and the confidentiality of the ballot.

3.1.7.2 No Recording of Alternate Format Usage

Voter anonymity shall be maintained for alternative format ballot presentation.

- a. No information shall be kept within an electronic cast vote record that identifies any alternative language feature(s) used by a voter.
- b. No information shall be kept within an electronic cast vote record that identifies any accessibility feature(s) used by a voter.

3.2 Accessibility Requirements

The voting process shall be accessible to voters with disabilities. As a minimum, every polling place shall have at least one voting station equipped for individuals with disabilities, as provided in HAVA 301 (a)(3)(B). A machine so equipped is referred to herein as an accessible voting station.

HAVA Section 301 (a) (3) reads, in part:

ACCESSIBILITY FOR INDIVIDUALS WITH DISABILITIES.--The voting system shall—

- (A) be accessible for individuals with disabilities, including nonvisual accessibility for the blind and visually impaired, in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters;**
(B) satisfy the requirement of subparagraph (A) through the use of at least one direct recording electronic voting system or other voting system equipped for individuals with disabilities at each polling place

The requirements in Subsection 3.2 are intended to address this mandate. Ideally, every voter would be able to vote independently and privately. As a practical matter, there may be some number of voters whose disabilities are so severe that they will need personal assistance. Nonetheless, these requirements are meant to make the voting system independently accessible to as many voters as possible. These requirements are in addition to those described in Subsection 3.1 Usability Requirements.

The outline for this subsection is:

- 3.2.1 General
- 3.2.2 Vision
- 3.2.3 Dexterity
- 3.2.4 Mobility
- 3.2.5 Hearing
- 3.2.6 Speech
- 3.2.7 English Proficiency
- 3.2.8 Cognition

3.2.1 General

The voting process shall incorporate the following features that are applicable to all types of disabilities:

- a. When the provision of accessibility involves an alternative format for ballot presentation, then all information presented to voters including instructions, warnings, error and other messages, and ballot choices shall be presented in that alternative format.
- b. The support provided to voters with disabilities shall be intrinsic to the accessible voting station. It shall not be necessary for the accessible voting station to be connected to any personal assistive device of the voter in order for the voter to operate it correctly.

Discussion: This requirement does not preclude the accessible voting station from providing interfaces to assistive technology. [See definition of “personal assistive devices” in the Glossary.] Its purpose is to assure that disabled voters are not required to bring special devices with them in order to vote successfully. The requirement does not assert that the accessible voting station will obviate the need for a voter’s ordinary non-interfacing devices, such as eyeglasses or canes. Jurisdictions should ensure that an accessible voting station provides clean and sanitary devices for voters with dexterity disabilities.

- c. When the primary means of voter identification or authentication uses biometric measures that require a voter to possess particular biological characteristics, the voting process shall provide a secondary means that does not depend on those characteristics.

Discussion: For example, if fingerprints are used for voter identification, another mechanism shall be provided for voters without usable fingerprints.

3.2.2 Vision

The voting process shall be accessible to voters with visual disabilities.

Discussion: Note that all aspects of the voting process are to be accessible, not just the voting machine.

3.2.2.1 Partial Vision

The accessible voting station shall be accessible to voters with partial vision.

- a. The vendor shall conduct summative usability tests on the voting system using partially sighted individuals. The vendor shall document the testing performed and report the test results using the Common Industry Format. This documentation shall be included in the Technical Data Package submitted to the EAC for national certification.

Discussion: Voting system developers are required to conduct realistic usability tests on the final product. For the present, vendors can define their own testing protocols. Future revisions to the *Guidelines* will include requirements for usability testing that will provide specific performance benchmarks.

- b. The accessible voting station with an electronic image display shall be capable of showing all information in at least two font sizes, (a) 3.0-4.0 mm and (b) 6.3-9.0 mm, under control of the voter.

Discussion: All millimeters will be calculated using Hard Metric Conversion. [See Glossary for definition.] While larger font sizes may assist most voters

with poor vision, certain disabilities such as tunnel vision are best addressed by smaller font sizes.

- c. An accessible voting station with a monochrome-only electronic image display shall be capable of showing all information in high contrast either by default or under the control of the voter or poll worker. High contrast is a figure-to-ground ambient contrast ratio for text and informational graphics of at least 6:1.
- d. An accessible voting station with a color electronic image display shall allow the voter to adjust the color or the figure-to-ground ambient contrast ratio.

Discussion: See Technical Guide for Color, Contrast and Text Size in Appendix D for examples of how a voting station may meet this requirement by offering a limited number of discrete choices. In particular, it is not required that the station offer a continuous range of color or contrast values.

- e. Buttons and controls on accessible voting stations shall be distinguishable by both shape and color.

Discussion: The redundant cues are helpful to those with low vision. They are also helpful to individuals who may have difficulty reading the text on the screen.

- f. An accessible voting station using an electronic image display shall provide synchronized audio output to convey the same information as that which is displayed on the screen.

3.2.2.2 Blindness

The accessible voting station shall be accessible to voters who are blind.

- a. The vendor shall conduct summative usability tests on the voting system using individuals who are blind. The vendor shall document the testing performed and report the test results using the Common Industry Format. This documentation shall be included in the Technical Data Package submitted to the EAC for national certification.

Discussion: Voting system developers are required to conduct realistic usability tests on the final product. For the present, vendors can define their own testing protocols. Future revisions to the *Guidelines* will include requirements for usability testing that will provide specific performance benchmarks.

- b. The accessible voting station shall provide an audio-tactile interface (ATI) that supports the full functionality of the visual ballot interface, as specified in Subsection 2.3.3.

Discussion: Note the necessity of both audio output and tactilely discernible controls for voter input. Full functionality includes at least:

- Instructions and feedback on initial activation of the ballot (such as insertion of a smart card), if this is normally performed by the voter on comparable voting stations
 - Instructions and feedback to the voter on how to operate the accessible voting station, including settings and options (e.g., volume control, repetition)
 - Instructions and feedback for navigation of the ballot
 - Instructions and feedback for contest choices, including write-in candidates
 - Instructions and feedback on confirming and changing selections
 - Instructions and feedback on final submission of ballot
- i. The ATI of the accessible voting station shall provide the same capabilities to vote and cast a ballot as are provided by other voting machines or by the visual interface of the standard voting machine.

Discussion: For example, if a visual ballot supports voting a straight party ticket and then changing the choice in a single contest, so must the ATI.

- ii. The ATI shall allow the voter to have any information provided by the voting system repeated.
- iii. The ATI shall allow the voter to pause and resume the audio presentation.
- iv. The ATI shall allow the voter to skip to the next contest or return to previous contests.

Discussion: This is analogous to the ability of sighted voters to move on to the next contest once they have made a selection or to abstain from voting on a contest altogether.

- v. The ATI shall allow the voter to skip over the reading of a referendum so as to be able to vote on it immediately.

Discussion: This is analogous to the ability of sighted voters to skip over the wording of a referendum on which they have already made a decision prior to the voting session (e.g., “Vote yes on proposition #123”).

- c. All voting stations that provide audio presentation of the ballot shall conform to the following requirements:

Discussion: These requirements apply to all voting machine audio output, not just to the ATI of an accessible voting station.

- i. The ATI shall provide its audio signal through an industry standard connector for private listening using a 3.5mm stereo headphone jack to allow voters to use their own audio assistive devices.

- ii. When a voting machine utilizes a telephone style handset or headphone to provide audio information, it shall provide a wireless T-Coil coupling for assistive hearing devices so as to provide access to that information for voters with partial hearing. That coupling shall achieve at least a category T4 rating as defined by American National Standard for Methods of Measurement of Compatibility between Wireless Communications Devices and Hearing Aids, ANSI C63.19.
- iii. No voting equipment shall cause electromagnetic interference with assistive hearing devices that would substantially degrade the performance of those devices. The voting equipment, considered as a wireless device, shall achieve at least a category T4 rating as defined by American National Standard for Methods of Measurement of Compatibility between Wireless Communications Devices and Hearing Aids, ANSI C63.19.

Discussion: "Hearing devices" include hearing aids and cochlear implants.

- iv. A sanitized headphone or handset shall be made available to each voter.

Discussion: This requirement can be achieved in various ways, including the use of "throwaway" headphones, or of sanitary coverings.

- v. The voting machine shall set the initial volume for each voter between 40 and 50 dB SPL.

Discussion: A voter does not "inherit" the volume as set by the previous user of the voting station.

- vi. The voting machine shall provide a volume control with an adjustable volume from a minimum of 20dB SPL up to a maximum of 100 dB SPL, in increments no greater than 10 dB.

- vii. The audio system shall be able to reproduce frequencies over the audible speech range of 315 Hz to 10 KHz.

- viii. The audio presentation of verbal information should be readily comprehensible by voters who have normal hearing and are proficient in the language. This includes such characteristics as proper enunciation, normal intonation, appropriate rate of speech, and low background noise. Candidate names should be pronounced as the candidate intends.

- ix. The audio system shall allow voters to control the rate of speech. The range of speeds supported should be at least 75% to 200% of the nominal rate.

Discussion: Many blind voters are accustomed to interacting with accelerated speech.

- d. If the normal procedure is to have voters initialize the activation of the ballot, the accessible voting station shall provide features that enable voters who are blind to perform this activation.

Discussion: For example, smart cards might provide tactile cues so as to allow correct insertion.

- e. If the normal procedure is for voters to submit their own ballots, then the accessible voting station shall provide features that enable voters who are blind to perform this submission.

Discussion: For example, if voters normally feed their own optical scan ballots into a reader, blind voters should also be able to do so.

- f. All mechanically operated controls or keys on an accessible voting station shall be tactilely discernible without activating those controls or keys.
- g. On an accessible voting station, the status of all locking or toggle controls or keys (such as the "shift" key) shall be visually discernible, and discernible either through touch or sound.

3.2.3 Dexterity

The voting process shall be accessible to voters who lack fine motor control or use of their hands.

- a. The vendor shall conduct summative usability tests on the voting system using individuals lacking fine motor control. The vendor shall document the testing performed and report the test results using the Common Industry Format. This documentation shall be included in the Technical Data Package submitted to the EAC for national certification.

Discussion: Voting system developers are required to conduct realistic usability tests on the final product. For the present, vendors can define their own testing protocols. Future revisions to the *Guidelines* will include requirements for usability testing that will provide specific performance benchmarks.

- b. All keys and controls on the accessible voting station shall be operable with one hand and shall not require tight grasping, pinching, or twisting of the wrist. The force required to activate controls and keys shall be no greater 5 lbs. (22.2 N).

Discussion: Controls are to be operable without excessive force.

- c. The accessible voting station controls shall not require direct bodily contact or for the body to be part of any electrical circuit.

Discussion: This requirement ensures that controls are operable by individuals using prosthetic devices.

- d. The accessible voting station shall provide a mechanism to enable non-manual input that is functionally equivalent to tactile input.

Discussion: This requirement ensures that the accessible voting station is operable by individuals who do not have the use of their hands. All the functionality of the accessible voting station (e.g., straight party voting, write-in candidates) that is available through the other forms of input, such as tactile, must also be available through a non-manual input mechanism if it is provided by the accessible voting station.

- e. If the normal procedure is for voters to submit their own ballots, then the accessible voting station shall provide features that enable voters who lack fine motor control or the use of their hands to perform this submission.

3.2.4 Mobility

The voting process shall be accessible to voters who use mobility aids, including wheelchairs.

- a. The accessible voting station shall provide a clear floor space of 30 inches (760 mm) minimum by 48 inches (1220 mm) minimum for a stationary mobility aid. The clear floor space shall be level with no slope exceeding 1:48 and positioned for a forward approach or a parallel approach.
- b. All controls, keys, audio jacks and any other part of the accessible voting station necessary for the voter to operate the voting machine shall be within reach as specified under the following sub-requirements:

Discussion: Note that these requirements have meaningful application mainly to controls in a fixed location. A hand-held tethered control panel is another acceptable way of providing reachable controls.

- i. If the accessible voting station has a forward approach with no forward reach obstruction then the high reach shall be 48 inches maximum and the low reach shall be 15 inches minimum. See Figure 1.
- ii. If the accessible voting station has a forward approach with a forward reach obstruction, the following requirements apply (See Figure 2):
- The forward obstruction shall be no greater than 25 inches in depth, its top no higher than 34 inches and its bottom surface no lower than 27 inches.
 - If the obstruction is no more than 20 inches in depth, then the maximum high reach shall be 48 inches, otherwise it shall be 44 inches.
- iii. Space under the obstruction between the finish floor or ground and 9 inches (230 mm) above the finish floor or ground shall be considered toe clearance and shall comply with the following provisions:

- Toe clearance shall extend 25 inches (635 mm) maximum under the obstruction
 - The minimum toe clearance under the obstruction shall be either 17 inches (430 mm) or the depth required to reach over the obstruction to operate the accessible voting station, whichever is greater
 - Toe clearance shall be 30 inches (760 mm) wide minimum
- iv. Space under the obstruction between 9 inches (230 mm) and 27 inches (685 mm) above the finish floor or ground shall be considered knee clearance and shall comply with the following provisions:
- Knee clearance shall extend 25 inches (635 mm) maximum under the obstruction at 9 inches (230 mm) above the finish floor or ground.
 - The minimum knee clearance at 9 inches (230 mm) above the finish floor or ground shall be either 11 inches (280 mm) or 6 inches less than the toe clearance, whichever is greater.
 - Between 9 inches (230 mm) and 27 inches (685 mm) above the finish floor or ground, the knee clearance shall be permitted to reduce at a rate of 1 inch (25 mm) in depth for each 6 inches (150 mm) in height.

Discussion: It follows that the minimum knee clearance at 27 inches above the finish floor or ground shall be 3 inches less than the minimum knee clearance at 9 inches above the floor.

- Knee clearance shall be 30 inches (760 mm) wide minimum.
- v. If the accessible voting station has a parallel approach with no side reach obstruction then the maximum high reach shall be 48 inches and the minimum low reach shall be 15 inches. See Figure 3.
- vi. If the accessible voting station has a parallel approach with a side reach obstruction, the following sub-requirements apply. See Figure 4.
- The side obstruction shall be no greater than 24 inches in depth and its top no higher than 34 inches.
 - If the obstruction is no more than 10 inches in depth, then the maximum high reach shall be 48 inches, otherwise it shall be 46 inches.

Discussion: Since this is a parallel approach, no clearance under the obstruction is required.

- c. All labels, displays, controls, keys, audio jacks, and any other part of the accessible voting station necessary for the voter to operate the voting machine shall be easily legible and visible to a voter in a wheelchair with normal eyesight (no worse than 20/40, corrected) who is in an appropriate position and orientation with respect to the accessible voting station

Discussion: There are a number of factors that could make relevant parts of the accessible voting station difficult to see such as; small lettering, controls and labels tilted at an awkward angle from the voter's viewpoint, and glare from overhead lighting.

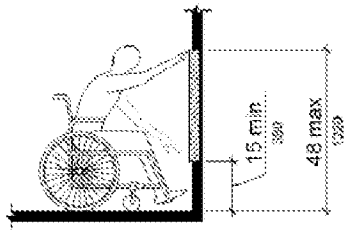
Figures 1-4

Figure 1
Unobstructed forward reach

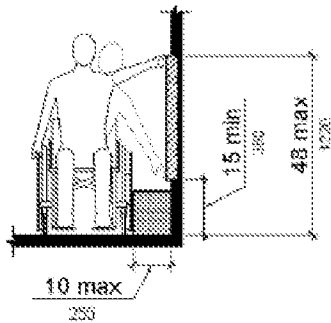


Figure 3
Unobstructed side reach with an allowable obstruction less than 10 inches (254 mm) deep.

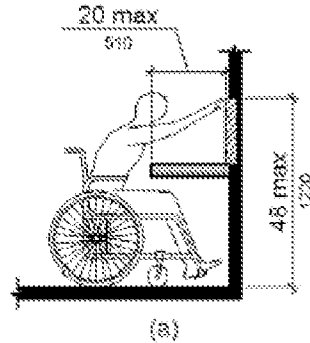
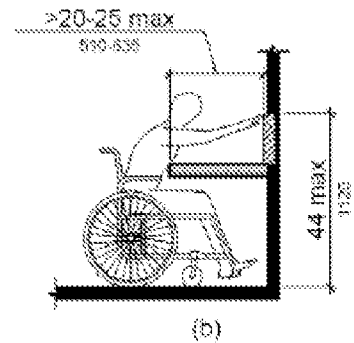


Figure 2
Obstructed forward reach
(a) for an obstruction depth of up to 20 inches (508 mm)
(b) for an obstruction depth of up to 25 inches (635 mm)

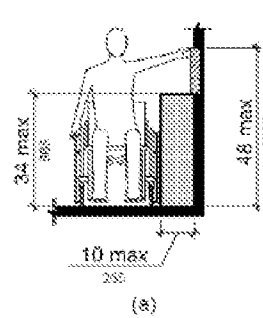
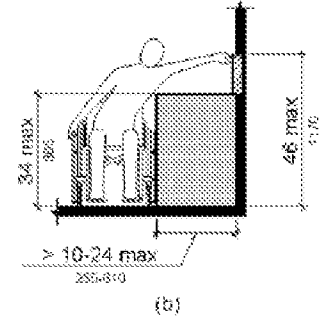


Figure 4
Obstructed side reach
(a) for an obstruction depth of up to 10 inches (254 mm)
(b) for an obstruction depth of up to 24 inches (610 mm)

3.2.5 Hearing

The voting process shall be accessible to voters with hearing disabilities.

- a. The accessible voting station shall incorporate the features listed under requirement 3.2.2.2 (c) for voting equipment that provides audio presentation of the ballot to provide accessibility to voters with hearing disabilities.

Discussion: Note especially the requirements for volume initialization and control.

- b. If voting equipment provides sound cues as a method to alert the voter, the tone shall be accompanied by a visual cue, unless the station is in audio-only mode.

Discussion: For instance, the voting equipment might beep if the voter attempts to overvote. If so, there would have to be an equivalent visual cue, such as the appearance of an icon, or a blinking element. Some voting equipment may have an audio-only mode, in which case, there would be no visual cue.

3.2.6 Speech

The voting process shall be accessible to voters with speech disabilities.

- a. No voting equipment shall require voter speech for its operation.

Discussion: This does not preclude voting equipment from offering speech input as an option, but speech must not be the only means of input.

3.2.7 English Proficiency

For voters who lack proficiency in reading English, or whose primary language is unwritten, the voting equipment shall provide spoken instructions and ballots in the preferred language of the voter, consistent with state and federal law. The requirements of 3.2.2.2 (c) shall apply to this mode of interaction.

3.2.8 Cognition

The voting process should be accessible to voters with cognitive disabilities.

Discussion: At present there are no design features specifically aimed at helping those with cognitive disabilities. Requirements 3.2.2.1 (f), the synchronization of audio with the screen in a DRE, is helpful for some cognitive disabilities such as dyslexia. Requirements in Subsection 3.1.4 also address cognitive issues relative to voting system usability.

4 Hardware Requirements

Table of Contents

4	Hardware Requirements.....	67
4.1	Performance Requirements.....	68
4.1.1	Accuracy Requirements.....	68
4.1.2	Environmental Requirements	70
4.1.2.1	Shelter Requirements.....	70
4.1.2.2	Space Requirements.....	70
4.1.2.3	Furnishings and Fixtures.....	70
4.1.2.4	Electrical Supply.....	71
4.1.2.5	Electrical Power Disturbance	71
4.1.2.6	Electrical Fast Transient	71
4.1.2.7	Lightning Surge	72
4.1.2.8	Electrostatic Disruption	72
4.1.2.9	Electromagnetic Emissions.....	72
4.1.2.10	Electromagnetic Susceptibility	72
4.1.2.11	Conducted RF Immunity	73
4.1.2.12	Magnetic Fields Immunity.....	73
4.1.2.13	Environmental Control - Operating Environment.....	73
4.1.2.14	Environmental Control - Transit and Storage.....	73
4.1.2.15	Data Network Requirements.....	74
4.1.3	Election Management System Requirements	74
4.1.3.1	Recording Requirements	74
4.1.3.2	Memory Stability	74
4.1.4	Vote Recording Requirements	75
4.1.4.1	Common Requirements	75
4.1.4.2	Paper-based Recording Requirements.....	75
4.1.4.3	DRE System Recording Requirements.....	77
4.1.5	Paper-based Conversion Requirements.....	78
4.1.5.1	Ballot Handling.....	78
4.1.5.2	Ballot Reading Accuracy	80
4.1.6	Tabulation Processing Requirements	80
4.1.6.1	Paper-based System Processing Requirements	80
4.1.6.2	DRE System Processing Requirements.....	81
4.1.7	Reporting Requirements.....	82
4.1.7.1	Removable Storage Media.....	82
4.1.7.2	Printers.....	82
4.1.8	Vote Data Management Requirements.....	82
4.1.8.1	Data File Management.....	83
4.1.8.2	Data Report Generation	83
4.2	Physical Characteristics.....	83
4.2.1	Size	83

4.2.2	Weight	84
4.2.3	Transport and Storage of Precinct Systems	84
4.3	Design, Construction, and Maintenance Characteristics	84
4.3.1	Materials, Processes, and Parts	84
4.3.2	Durability	85
4.3.3	Reliability	85
4.3.4	Maintainability	85
4.3.4.1	Physical Attributes	86
4.3.4.2	Additional Attributes	86
4.3.5	Availability	86
4.3.6	Product Marking	88
4.3.7	Workmanship	88
4.3.8	Safety	88

4 Hardware Requirement

This section contains the requirements for the machines and manufactured devices that are part of a voting system. It specifies minimum values for certain performance characteristics; physical characteristics; and design, construction, and maintenance characteristics for the hardware and selected related components of all voting systems, such as:

- Ballot printers
- Ballot cards and sheets
- Ballot displays
- Voting devices, including ballot marking devices and DRE recording devices
- Voting booths and enclosures
- Ballot boxes and ballot transfer boxes
- Ballot readers
- Computers used to prepare ballots, program elections, consolidate and report votes, and perform other elections management activities
- Electronic ballot recorders
- Electronic precinct vote control units
- Removable electronic data storage media
- Servers
- Printers

This section applies to the combination of software and hardware to accomplish specific performance and system control requirements. Standards that are specific to software alone are provided in Section 5.

The requirements of this section apply generally to all hardware used in voting systems, including:

- Hardware provided by the voting system vendor and its suppliers
- Hardware furnished by an external provider (for example, providers of commercial-off-the-shelf equipment) where the hardware may be used in any way during voting system operation
- Hardware provided by the voting jurisdiction

The requirements presented in this section are organized as follows:

Performance Requirements: These requirements address the combined operational capabilities of the voting system hardware and software across a broad range of parameters

Physical Requirements: These requirements address the size, weight and transportability of the voting system

Design, Construction, and Maintenance Requirements: These requirements address the reliability and durability of materials, product marking, quality of system workmanship, safety, and other attributes to ensure smooth system operation in the voting environment

4.1 Performance Requirements

The performance requirements address a broad range of parameters, encompassing:

- Accuracy requirements, where requirements are specified for distinct processing functions of paper-based and DRE systems
- Environmental requirements, where no distinction is made between requirements for paper-based and DRE systems, but requirements for precinct and central count are described
- Vote data management requirements, where no differentiation is made between requirements for paper-based and DRE systems
- Vote recording requirements, where separate and distinct requirements are delineated for paper-based and DRE systems
- Conversion requirements, which apply only to paper-based systems
- Processing requirements, where separate and distinct requirements are delineated for paper-based and DRE systems
- Reporting requirements, where no distinction is made between requirements for paper-based and DRE systems, but where differences between precinct and central count systems are readily apparent based on differences of their reporting

The performance requirements include such attributes as ballot reading and handling requirements; system accuracy; memory stability; and the ability to withstand specified environmental conditions. These characteristics also encompass system-wide requirements for shelter, electrical supply, and compatibility with data networks.

Performance requirements for voting systems represent the combined operational capability of both system hardware and software. Accuracy, as measured by data error rate, and operational failure are treated as distinct attributes in performance testing. All systems shall meet the performance requirements under operating conditions and after storage under non-operating conditions.

4.1.1 Accuracy Requirements

Voting system accuracy addresses the accuracy of data for each of the individual ballot positions that could be selected by a voter, including the positions that are not selected. For a voting system, accuracy is defined as the ability of the system to capture, record, store, consolidate and report the specific selections and absence of selections, made by the voter for each ballot position without error. Required accuracy is defined in terms of an error rate that for testing purposes represents the maximum number of errors allowed while processing a

specified volume of data. This rate is set at a sufficiently stringent level that the likelihood of voting system errors affecting the outcome of an election is exceptionally remote even in the closest of elections.

The error rate is defined using a convention that recognizes differences in how vote data is processed by different types of voting systems. Paper-based and DRE systems have different processing steps. Some differences also exist between precinct count and central count systems. Therefore, the acceptable error rate applies separately and distinctly to each of the following functions:

- a. For all paper-based voting systems:
 - i. Scanning ballot positions on paper ballots to detect selections for individual candidates and contests
 - ii. Conversion of selections detected on paper ballots into digital data
- b. For all DRE voting systems:
 - i. Recording the voter selections of candidates and contests into voting data storage
 - ii. Recording voter selections of candidates and contests into ballot image storage independently from voting data storage
- c. For precinct-count voting systems (paper-based and DRE):
 - i. Consolidation of vote selection data from multiple precinct-based voting machines to generate jurisdiction-wide vote counts, including storage and reporting of the consolidated vote data
- d. For central-count voting systems (paper-based and DRE):
 - i. Consolidation of vote selection data from multiple counting devices to generate jurisdiction-wide vote counts, including storage and reporting of the consolidated vote data

For testing purposes, the acceptable error rate is defined using two parameters: the desired error rate to be achieved, and the maximum error rate that should be accepted by the test process.

For each processing function indicated above, the voting system shall achieve a target error rate of no more than one in 10,000,000 ballot positions, with a maximum acceptable error rate in the test process of one in 500,000 ballot positions.

4.1.2 Environmental Requirements

The environmental requirements for voting systems include shelter, space, furnishings and fixtures, supplied energy, environmental control, and external telecommunications services. Environmental conditions applicable to the design and operation of voting systems consist of the following categories:

- Natural environment, including temperature, humidity, and atmospheric pressure
- Induced environment, including proper and improper operation and handling of the system and its components during the election processes
- Transportation and storage
- Electromagnetic signal environment, including exposure to and generation of radio frequency energy

All voting systems shall be designed to withstand the environmental conditions contained in the appropriate test procedures of the *Guidelines*. These procedures will be applied to all devices for casting, scanning and counting ballots, except those that constitute COTS devices that have not been modified in any manner to support their use as part of a voting system and that have a documented record of performance under conditions defined in the *Guidelines*.

The Technical Data Package supplied by the vendor shall include a statement of all requirements and restrictions regarding environmental protection, electrical service, recommended auxiliary power, telecommunications service, and any other facility or resource required for the proper installation and operation of the system.

4.1.2.1 Shelter Requirements

All precinct count systems shall be designed for storage and operation in any enclosed facility ordinarily used as a warehouse or polling place, with prominent instructions as to any special storage requirements.

4.1.2.2 Space Requirements

There is no restriction on space allowed for the installation of voting systems, except that the arrangement of these systems shall not impede performance of their duties by polling place officials, the orderly flow of voters through the polling place or the ability for the voter to vote in private.

4.1.2.3 Furnishings and Fixtures

Any furnishings or fixtures provided as a part of voting systems, and any components provided by the vendor that are not a part of the voting system but that are used to support its storage, transportation or operation, shall comply with the safety design of Subsection 4.3.8.

4.1.2.4 Electrical Supply

Components of voting systems that require an electrical supply shall meet the following standards:

- a. Precinct count voting systems shall operate with the electrical supply ordinarily found in polling places (Nominal 120 Vac/60Hz/1 phase)
- b. Central count voting systems shall operate with the electrical supply ordinarily found in central tabulation facilities or computer room facilities (Nominal 120 Vac/60Hz/1, nominal 208 Vac/60Hz/3 or nominal 240 Vac/60Hz/2)
- c. All voting machines shall also be capable of operating for a period of at least 2 hours on backup power, such that no voting data is lost or corrupted nor normal operations interrupted. When backup power is exhausted the voting machine shall retain the contents of all memories intact

The backup power capability is not required to provide lighting of the voting area.

4.1.2.5 Electrical Power Disturbance

Vote scanning and counting equipment for paper-based voting systems, and all DRE voting equipment, shall be able to withstand, without disruption of normal operation or loss of data:

- a. Voltage dip of 30% of nominal @10 ms;
- b. Voltage dip of 60% of nominal @100 ms & 1 sec
- c. Voltage dip of >95% interrupt @5 sec
- d. Surges of $\pm 15\%$ line variations of nominal line voltage
- e. Electric power increases of 7.5% and reductions of 12.5% of nominal specified power supply for a period of up to four hours at each power level

4.1.2.6 Electrical Fast Transient

Vote scanning and counting equipment for paper-based systems, and all DRE equipment, shall be able to withstand, without disruption of normal operation or loss of data, electrical fast transients of:

- a. + 2 kV and - 2 kV on External Power lines (both AC and DC)
- b. + 1 kV and - 1 kV on Input/Output lines(signal, data, and control lines) longer than 3 meters

- c. Repetition Rate for all transient pulses will be 100 kHz

4.1.2.7 Lightning Surge

Vote scanning and counting equipment for paper-based systems, and all DRE equipment, shall be able to withstand, without disruption of normal operation or loss of data, surges of:

- a. ± 2 kV AC line to line
- b. ± 2 kV AC line to earth
- c. + or – 0.5 kV DC line to line >10m
- d. + or – 0.5 kV DC line to earth >10m
- e. ± 1 kV I/O sig/control >30m

4.1.2.8 Electrostatic Disruption

Vote scanning and counting equipment for paper-based systems, and all DRE equipment, shall be able to withstand ± 15 kV air discharge and ± 8 kV contact discharge without damage or loss of data. The equipment may reset or have momentary interruption so long as normal operation is resumed without human intervention or loss of data. Loss of data means votes that have been completed and confirmed to the voter.

4.1.2.9 Electromagnetic Emissions

Vote scanning and counting equipment for paper-based systems, and all DRE equipment, shall comply with the Rules and Regulations of the Federal Communications Commission, Part 15; Class B requirements for both radiated and conducted emissions.

4.1.2.10 Electromagnetic Susceptibility

Vote scanning and counting equipment for paper-based systems, and all DRE equipment, shall be able to withstand an electromagnetic field of 10 V/m modulated by a 1 kHz 80% AM modulation over the frequency range of 80 MHz to 1000 MHz, without disruption of normal operation or loss of data.

4.1.2.11 Conducted RF Immunity

Vote scanning and counting equipment for paper-based systems, and all DRE equipment, shall be able to withstand, without disruption of normal operation or loss of data, conducted RF energy of:

- a. 10V rms over the frequency range 150 KHz to 80 MHz with an 80% amplitude modulation with a 1 KHz sine wave AC & DC power
- b. 10V sig/control >3 m over the frequency range 150 KHz to 80 MHz with an 80% amplitude modulation with a 1 KHz sine wave

4.1.2.12 Magnetic Fields Immunity

Vote scanning and counting equipment for paper-based systems, and all DRE equipment, shall be able to withstand, without disruption of normal operation or loss of data, AC magnetic fields of 30 A/m at 60 Hz.

4.1.2.13 Environmental Control - Operating Environment

Equipment used for election management activities or vote counting (including both precinct and central count systems) shall be capable of operation in temperatures ranging from 50 to 95 degrees Fahrenheit.

4.1.2.14 Environmental Control - Transit and Storage

Equipment used for vote casting or for counting votes in a precinct count system, shall meet these specific minimum performance standards that simulate exposure to physical shock and vibration associated with handling and transportation by surface and air common carriers, and to temperature conditions associated with delivery and storage in an uncontrolled warehouse environment:

- a. High and low storage temperatures ranging from -4 to +140 degrees Fahrenheit, equivalent to MIL-STD-810D, Methods 501.2 and 502.2, Procedure I-Storage
- b. Bench handling equivalent to the procedure of MIL-STD-810D, Method 516.3, Procedure VI
- c. Vibration equivalent to the procedure of MIL-STD-810D, Method 514.3, Category 1-Basic Transportation, Common Carrier
- d. Uncontrolled humidity equivalent to the procedure of MIL-STD-810D, Method 507.2, Procedure I-Natural Hot-Humid

4.1.2.15 Data Network Requirements

Voting systems may use a local or remote data network. If such a network is used, then all components of the network shall comply with the telecommunications requirements described in Section 6 and the Security requirements described in Section 7.

4.1.3 Election Management System Requirements

The Election Management System (EMS) requirements address electronic hardware and software used to conduct the pre-voting functions defined in Section 2 with regard to ballot preparation, election programming, ballot and program installation, readiness testing, verification at the polling place, and verification at the central location.

4.1.3.1 Recording Requirements

Voting systems shall accurately record all election management data entered by the user, including election officials or their designees.

For recording accuracy, all systems shall:

- a. Record every entry made by the user
- b. Add permissible voter selections correctly to the memory components of the device
- c. Verify the correctness of detection of the user selections and the addition of the selections correctly to memory
- d. Add various forms of data entered directly by the election official or designee, such as text, line art, logos, and images
- e. Verify the correctness of detection of data entered directly by the user and the addition of the selections correctly to memory
- f. Preserve the integrity of election management data stored in memory against corruption by stray electromagnetic emissions, and internally generated spurious electrical signals
- g. Log corrected data errors by the voting system

4.1.3.2 Memory Stability

Memory devices used to retain election management data shall have demonstrated error-free data retention for a period of 22 months.

4.1.4 Vote Recording Requirements

The vote recording requirements address the enclosure, equipment, and supplies used by voters to vote.

4.1.4.1 Common Requirements

All voting systems shall provide voting booths or enclosures for poll site use. Such booths or enclosures may be integral to the voting system or supplied as components of the voting system, and shall:

- a. Be integral to, or make provision for, the installation of the voting machine
- b. Ensure by its structure stability against movement or overturning during entry, occupancy, and exit by the voter
- c. Provide privacy for the voter, and be designed in such a way as to prevent observation of the ballot by any person other than the voter
- d. Be capable of meeting the accessibility requirements of Subsection 3.2

4.1.4.2 Paper-based Recording Requirements

The paper-based recording requirements govern:

- Ballot cards or sheets, and pages or assemblies of pages containing ballot field identification data
 - Ballot marking devices
 - Frames or fixtures to hold the ballot while it is being marked
 - Compartments or booths where voters record selections
 - Secure containers for the collection of voted ballots
- a. Paper ballots used by paper-based voting systems shall meet the following standards:
 - i. Marks that identify the unique ballot format shall be outside the area in which votes are recorded, so as to minimize the likelihood that these marks will be mistaken for vote responses and the likelihood that recorded votes will obliterate these marks
 - ii. If printed alignment marks are used to locate the vote response fields on the ballot, these marks shall be outside the area in which votes are recorded, so as to minimize the likelihood that these marks will be mistaken for vote responses and the likelihood that recorded votes will obliterate these marks

- iii. The Technical Data Package shall specify the required paper stock, size, shape, opacity, color, watermarks, field layout, orientation, size and style of printing, size and location of mark fields used for vote response fields and to identify unique ballot formats, placement of alignment marks, ink for printing, and folding and bleed-through limitations for preparation of ballots that are compatible with the system
- b. The Technical Data Package shall specify marking devices, which, if used to make the prescribed form of mark, produce readable marked ballots such that the system meets the performance requirements for accuracy in Subsection 4.1.1. Marking devices can be either manual (such as pens or pencils) or electronic. These specifications shall identify:
 - i. Specific characteristics of marking devices that affect readability of marked ballots
 - ii. Performance capabilities with regard to each characteristic
 - iii. For marking devices manufactured by multiple external sources, a listing of sources and model numbers that are compatible with the system
- c. A frame or fixture for printed ballot cards is optional. However, if such a device is provided, it shall:
 - i. Be of any size and shape consistent with its intended use
 - ii. Position the card properly
 - iii. Hold the ballot card securely in its proper location and orientation for voting
 - iv. Comply with the requirements for design and construction contained in Subsection 4.3
- d. Ballot boxes and ballot transfer boxes, which serve as secure containers for the storage and transportation of voted ballots, shall:
 - i. Be of any size, shape, and weight commensurate with their intended use
 - ii. Incorporate locks or seals, the specifications of which are described in the system documentation
 - iii. Provide specific points where ballots are inserted, with all other points on the box constructed in a manner that prevents ballot insertion
 - iv. For precinct count systems, contain separate compartments for the segregation of unread ballots, ballots containing write-in votes or any irregularities that may require special handling or processing. In lieu of compartments, the conversion

processing may mark such ballots with an identifying spot or stripe to facilitate manual segregation

4.1.4.3 DRE System Recording Requirements

The DRE system recording requirements address the detection and recording of votes, including the logic and data processing functions required to determine the validity of voter selections, to accept and record valid selections, and to reject invalid selections. The requirements also address the physical environment in which ballots are cast.

- a. DRE systems shall include an audible or visible activity indicator providing the status of each voting device. This indicator shall:
 - i. Indicate whether the device has been activated for voting
 - ii. Indicate whether the device is in use
- b. To ensure vote recording accuracy and integrity while protecting the anonymity of the voter, all DRE systems shall:
 - i. Contain all mechanical, electromechanical, and electronic components; software; and controls required to detect and record the activation of selections made by the voter in the process of voting and casting a ballot
 - ii. Incorporate redundant memories to detect and allow correction of errors caused by the failure of any of the individual memories
 - iii. Provide at least two processes that record the voter's selections that:
 - To the extent possible, are isolated from each other
 - Designate one process and associated storage location as the main vote detection, interpretation, processing and reporting path
 - iv. Use a different process to store ballot images, for which the method of recording may include any appropriate encoding or data compression procedure consistent with the regeneration of an unequivocal record of the ballot as cast by the voter
 - v. Provide a capability to retrieve ballot images in a form readable by humans
 - vi. Ensure that all processing and storage protects the anonymity of the voter
- c. DRE systems shall meet the following requirements for recording accurately each vote and ballot cast:
 - i. Detect every selection made by the voter

- ii. Correctly add permissible selections to the memory components of the device
- iii. Verify the correctness of the detection of the voter selections and the addition of the selections to memory
- iv. Achieve an error rate not to exceed the requirement indicated in Subsection 4.1.1
- v. Preserve the integrity of voting data and ballot images (for DRE machines) stored in memory for the official vote count and audit trail purposes against corruption by stray electromagnetic emissions, and internally generated spurious electrical signals
- vi. Maintain a log of corrected data

Recording reliability refers to the ability of the DRE system to record votes accurately at its maximum rated processing volume for a specified period of time. The DRE system shall record votes reliably in accordance with the requirements of Subsection 4.3.3.

4.1.5 Paper-based Conversion Requirements

The paper-based conversion requirements address the ability of the system to read the ballot card and to translate its pattern of marks into electronic signals for later processing. These capabilities may be built into the voting system in an integrated fashion, or may be provided by one or more components that are not unique to the system, such as a general purpose data processing card reader or read head suitably interfaced to the system. These requirements address two major functions: ballot handling and ballot reading.

4.1.5.1 Ballot Handling

Ballot handling consists of a ballot card's acceptance, movement through the read station, and transfer into a collection station or receptacle.

- a. The capacity to convert the marks on individual ballots into signals is uniquely important to central count systems. The capacity for a central count system shall be documented by the vendor. This documentation shall include the capacity for individual components that impact the overall capacity
- b. When ballots are unreadable or some condition is detected requiring that the cards be segregated from normally processed ballots for human review (e.g. write-ins), all central count paper-based systems shall do one of the following:
 - i. Outstack the ballot

- ii. Stop the ballot reader and display a message prompting the election official or designee to remove the ballot
 - iii. Mark the ballot with an identifying mark to facilitate its later identification
- c. Additionally, the system shall provide a capability that can be activated by an authorized election official to identify ballots containing overvotes, blank ballots, and ballots containing undervotes in a designated contest. If enabled, these capabilities shall perform one of the above actions in response to the indicated condition.
- d. When ballots are unreadable or when some condition is detected requiring that the cards be segregated from normally processed ballots for human review (e.g. write-in votes) all precinct count systems shall:
 - i. In response to an unreadable or blank ballot, return the ballot and provide a message prompting the voter to examine the ballot
 - ii. In response to a ballot with a write-in vote, segregate the ballot or mark the ballot with an identifying mark to facilitate its later identification
 - iii. In response to a ballot with an overvote the system shall:
 - Provide a capability to identify an overvoted ballot
 - Return the ballot
 - Provide an indication prompting the voter to examine the ballot
 - Allow the voter to correct the ballot
 - Provide a means for an authorized election official to deactivate this capability entirely and by contest
 - iv. In response to a ballot with an undervote, the system shall:
 - Provide a capability to identify an undervoted ballot
 - Return the ballot
 - Provide an indication prompting the voter to examine the ballot
 - Allow the voter to correct the ballot
 - Allow the voter to submit the ballot with the undervote
 - Provide a means for an authorized election official to deactivate this capability
- e. Ballot readers shall prevent multiple feed or detect and provide an alarm indicating multiple feed. Multiple feed occurs when a ballot reader attempts to read more than one ballot at a time.
 - i. If multiple feed is detected, the card reader shall halt in a manner that permits the operator to remove the unread cards causing the error, and reinsert them in the card input hopper

- ii. The frequency of multiple feeds with ballots intended for use with the system shall not exceed 1 in 10,000

4.1.5.2 Ballot Reading Accuracy

This paper-based system requirement governs the conversion of the physical ballot into electronic data. Reading accuracy for ballot conversion refers to the ability to:

- a. Recognize vote punches or marks, or the absence thereof, for each possible selection on the ballot
- b. Discriminate between valid punches or marks and extraneous perforations, smudges, and folds
- c. Convert the vote punches or marks, or the absence thereof, for each possible selection on the ballot into digital signals

To ensure accuracy, paper-based systems shall:

- d. Detect punches or marks that conform to vendor specifications with an error rate not exceeding the requirement indicated in Subsection 4.1.1
- e. Ignore, and not record, extraneous perforations, smudges, and folds
- f. Reject ballots that meet all vendor specifications at a rate not to exceed 2 percent

4.1.6 Tabulation Processing Requirements

Tabulation processing requirements apply to the hardware and software required to accumulate voting data for all candidates and measures within voting machines and polling places, and to consolidate the voting data at a central level or multiple levels. These requirements also address the generation and maintenance of audit records, the detection and disabling of improper use or operation of the system, and the monitoring of overall system status. Separate and distinct requirements for paper-based and DRE voting systems are presented below.

4.1.6.1 Paper-based System Processing Requirements

The paper-based processing requirements address all mechanical devices, electromechanical devices, electronic devices, and software required to perform the logical and numerical functions of interpreting the electronic image of the voted ballot, and assigning votes to the proper memory registers.

- a. Processing accuracy refers to the ability of the system to receive electronic signals produced by punches for punchcard systems and vote marks and timing information for marksense systems; perform logical and numerical operations upon these data; and reproduce the contents of memory when required, without error. Specific requirements are detailed below:
 - i. Processing accuracy shall be measured by vote selection error rate, the ratio of uncorrected vote selection errors to the total number of ballot positions that could be recorded across all ballots when the system is operated at its nominal or design rate of processing
 - ii. The vote selection error rate shall include data that denotes ballot style or precinct as well as data denoting a vote in a specific contest or ballot proposition
 - iii. The vote selection error rate shall include all errors from any source
 - iv. The vote selection error rate shall not exceed the requirement indicated in Subsection 4.1.1
- b. Paper-based system memory devices, used to retain control programs and data, shall have demonstrated error-free data retention for a period of 22 months, under the environmental conditions for operation and non-operation (i.e., storage).

4.1.6.2 DRE System Processing Requirements

The DRE voting systems processing requirements address all mechanical devices, electromechanical devices, electronic devices, and software required to process voting data after the polls are closed.

- a. DRE voting systems shall meet the following requirements for processing speed:
 - i. Operate at a speed sufficient to respond to any operator and voter input without perceptible delay (no more than three seconds)
 - ii. If the consolidation of polling place data is done locally, perform this consolidation in a time not to exceed five minutes for each device in the polling place
- b. Processing accuracy is defined as the ability of the system to process voting data stored in DRE voting devices or in removable memory modules installed in such devices. Processing includes all operations to consolidate voting data after the polls have been closed. DRE voting systems shall:
 - i. Produce reports that are completely consistent, with no discrepancy among reports of voting device data produced at any level

- ii. Produce consolidated reports containing absentee, provisional or other voting data that are similarly error-free. Any discrepancy, regardless of source, is resolvable to a procedural error, to the failure of a non-memory device or to an external cause
- c. DRE system memory devices used to retain control programs and data shall have demonstrated error-free data retention for a period of 22 months. Error-free retention may be achieved by the use of redundant memory elements, provided that the capability for conflict resolution or correction among elements is included.

4.1.7 Reporting Requirements

The reporting requirements govern all mechanical, electromechanical, and electronic devices required for voting systems to print audit record entries and results of the tabulation. These requirements also address data storage media for transportation of data to other sites.

4.1.7.1 Removable Storage Media

In voting systems that use storage media that can be removed from the system and transported to another location for readout and report generation, these media shall use devices with demonstrated error-free retention for a period of 22 months under the environmental conditions for operation and non-operation contained in Subsection 4.1.2. Examples of removable storage media include: programmable read-only memory (PROM), random access memory (RAM) with battery backup, magnetic media or optical media.

4.1.7.2 Printers

All printers used to produce reports of the vote count shall be capable of producing:

- a. Alphanumeric headers
- b. Election, office and issue labels
- c. Alphanumeric entries generated as part of the audit record

4.1.8 Vote Data Management Requirements

The vote data management requirements for all systems address capabilities that manage, process, and report voting data after the data has been consolidated at the polling place or other jurisdictional levels.

These capabilities allow the system to:

- Consolidate voting data from polling place data memory or transfer devices
- Report polling place summaries
- Process absentee ballots, data entered manually, and administrative ballot definition data

The requirements address all hardware and software required to generate output reports in the various formats required by the using jurisdiction.

4.1.8.1 Data File Management

All voting systems shall provide the capability to:

- a. Integrate voting data files with ballot definition files
- b. Verify file compatibility
- c. Edit and update files as required

4.1.8.2 Data Report Generation

All voting systems shall include report generators for producing output reports at the device, polling place, and summary level, with provisions for administrative and judicial subdivisions as required by the using jurisdiction.

4.2 Physical Characteristics

This subsection covers physical characteristics of all voting systems and components that affect their general utility and suitability for election operations.

4.2.1 Size

There is no numerical limitation on the size of any voting equipment, but the size of each voting machine should be compatible with its intended use and the location at which the equipment is to be used.

4.2.2 Weight

There is no numerical limitation on the weight of any voting equipment, but the weight of each voting machine should be compatible with its intended use and the location at which the equipment is to be used.

4.2.3 Transport and Storage of Precinct Systems

All precinct voting systems shall:

- a. Provide a means to safely and easily handle, transport, and install voting equipment, such as wheels or a handle or handles
- b. Be capable of using, or be provided with, a protective enclosure rendering the equipment capable of withstanding:
 - i. Impact, shock and vibration loads associated with surface and air transportation
 - ii. Stacking loads associated with storage

4.3 Design, Construction, and Maintenance Characteristics

This subsection covers voting system materials, construction workmanship, and specific design characteristics important to the successful operation and efficient maintenance of the voting system.

4.3.1 Materials, Processes, and Parts

The approach to system design is unrestricted, and may incorporate any form or variant of technology capable of meeting the voting systems requirements and standards.

Precinct count systems shall be designed in accordance with best commercial practice for microcomputers, process controllers, and their peripheral components. Central count voting systems and equipment used in a central tabulating environment shall be designed in accordance with best commercial and industrial practice.

All voting systems shall:

- a. Be designed and constructed so that the frequency of equipment malfunctions and maintenance requirements are reduced to the lowest level consistent with cost constraints
- b. Include, as part of the accompanying Technical Data Package, an approved parts list

- c. Exclude parts or components not included in the approved parts list

4.3.2 Durability

All voting systems shall be designed to withstand normal use without deterioration and without excessive maintenance cost for a period of ten years.

4.3.3 Reliability

The reliability of voting system devices shall be measured as Mean Time Between Failure (MTBF) for the system submitted for testing. MTBF is defined as the value of the ratio of operating time to the number of failures which have occurred in the specified time interval. A typical system operations scenario consists of approximately 45 hours of equipment operation, consisting of 30 hours of equipment set-up and readiness testing and 15 hours of elections operations. For the purpose of demonstrating compliance with this requirement, a failure is defined as any event which results in either the:

- Loss of one or more functions
- Degradation of performance such that the device is unable to perform its intended function for longer than 10 seconds

The MTBF demonstrated during certification testing shall be at least 163 hours.

4.3.4 Maintainability

Maintainability represents the ease with which maintenance actions can be performed based on the design characteristics of equipment and software and the processes the vendor and election officials have in place for preventing failures and for reacting to failures. Maintainability includes the ability of equipment and software to self-diagnose problems and make non-technical election workers aware of a problem. Maintainability addresses all scheduled and unscheduled events, which are performed to:

- Determine the operational status of the system or a component
- Adjust, align, tune or service components
- Repair or replace a component having a specified operating life or replacement interval
- Repair or replace a component that exhibits an undesirable predetermined physical condition or performance degradation
- Repair or replace a component that has failed
- Verify the restoration of a component or the system to operational status

Maintainability shall be determined based on the presence of specific physical attributes that aid system maintenance activities, and the ease with which system maintenance tasks can be

performed by the test lab. Although a more quantitative basis for assessing maintainability, such as the Mean Time to Repair the system is desirable, the certification of a system is conducted before it is approved for sale and thus before a broader base of maintenance experience can be obtained.

4.3.4.1 Physical Attributes

The following physical attributes will be examined to assess reliability:

- a. Presence of labels and the identification of test points
- b. Provision of built-in test and diagnostic circuitry or physical indicators of condition
- c. Presence of labels and alarms related to failures
- d. Presence of features that allow non-technicians to perform routine maintenance tasks (such as update of the system database)

4.3.4.2 Additional Attributes

The following additional attributes will be considered to assess system maintainability:

- a. Ease of detecting that equipment has failed by a non-technician
- b. Ease of diagnosing problems by a trained technician
- c. Low false alarm rates (i.e., indications of problems that do not exist)
- d. Ease of access to components for replacement
- e. Ease with which adjustment and alignment can be performed
- f. Ease with which database updates can be performed by a non-technician
- g. Adjust, align, tune or service components

4.3.5 Availability

The availability of a voting system is defined as the probability that the equipment (and supporting software) needed to perform designated voting functions will respond to operational commands and accomplish the function. The voting system shall meet the availability standard for each of the following voting functions:

- a. For all paper-based systems:

- i. Recording voter selections (such as by ballot marking or punch)
 - ii. Scanning the punches or marks on paper ballots and converting them into digital data
- b. For all DRE systems, recording and storing voter ballot selections
 - c. For precinct count systems (paper-based and DRE), consolidation of vote selection data from multiple precinct based systems to generate jurisdiction-wide vote counts, including storage and reporting of the consolidated vote data
 - d. For central-count systems (paper-based and DRE), consolidation of vote selection data from multiple counting devices to generate jurisdiction-wide vote counts, including storage and reporting of the consolidated vote data

System availability is measured as the ratio of the time during which the system is operational (up time) to the total time period of operation (up time plus down time). Inherent availability (A_i) is the fraction of time a system is functional, based upon Mean Time Between Failure (MTBF) and Mean Time To Repair (MTTR), that is:

$$A_i = (\text{MTBF})/(\text{MTBF} + \text{MTTR})$$

MTTR is the average time required to perform a corrective maintenance task during periods of system operation. Corrective maintenance task time is active repair time, plus the time attributable to other factors that could lead to logistic or administrative delays, such as travel notification of qualified maintenance personnel and travel time for such personnel to arrive at the appropriate site.

Corrective maintenance may consist of substitution of the complete device or one of its components, as in the case of precinct count and some central count systems, or it may consist of on-site repair.

The voting system shall achieve at least 99 percent availability during normal operation for the functions indicated above. This standard encompasses for each function the combination of all devices and components that support the function, including their MTTR and MTBF attributes.

Vendors shall specify the typical system configuration that is to be used to assess availability, and any assumptions made with regard to any parameters that impact the MTTR. These factors shall include at a minimum:

- e. Recommended number and locations of spare devices or components to be kept on hand for repair purposes during periods of system operation
- f. Recommended number and locations of qualified maintenance personnel who need to be available to support repair calls during system operation

- g. Organizational affiliation (i.e., jurisdiction, vendor) of qualified maintenance personnel

4.3.6 Product Marking

All voting systems shall:

- a. Identify all devices by means of a permanently affixed nameplate or label containing the name of the manufacturer or vendor, the name of the device, its part or model number, its revision letter, its serial number, and if applicable, its power requirements
- b. Display on each device a separate data plate containing a schedule for and list of operations required to service or to perform preventive maintenance
- c. Display advisory caution and warning instructions to ensure safe operation of the equipment and to avoid exposure to hazardous electrical voltages and moving parts at all locations where operation or exposure may occur

4.3.7 Workmanship

To help ensure proper workmanship, all manufacturers of voting systems shall:

- a. Adopt and adhere to practices and procedures to ensure that their products are free from damage or defect that could make them unsatisfactory for their intended purpose
- b. Ensure that components provided by external suppliers are free from damage or defect that could make them unsatisfactory for their intended purpose

4.3.8 Safety

All voting systems shall meet the following requirements for safety:

- a. All voting systems and their components shall be designed to eliminate hazards to personnel or to the equipment itself
- b. Defects in design and construction that can result in personal injury or equipment damage must be detected and corrected before voting systems and components are placed into service
- c. Equipment design for personnel safety shall be equal to or better than the appropriate requirements of the Occupational Safety and Health Act, Code of Federal Regulations, Title 29, Part 1910

5 Software Requirements

Table of Contents

5	Software Requirements.....	91
5.1	Scope	91
5.1.1	Software Sources.....	91
5.1.2	Management of Software and Hardware	92
5.1.3	Exclusions.....	92
5.2	Software Design and Coding Standards	93
5.2.1	Selection of Programming Languages.....	93
5.2.2	Software Integrity	93
5.2.3	Software Modularity and Programming	94
5.2.4	Control Constructs.....	95
5.2.5	Naming Conventions.....	95
5.2.6	Coding Conventions	96
5.2.7	Comment Conventions	96
5.3	Data and Document Retention	97
5.4	Audit Record Data	97
5.4.1	Pre-election Audit Records.....	98
5.4.2	System Readiness Audit Records.....	98
5.4.3	In-process Audit Records	99
5.4.4	Vote Tally Data	100
5.5	Vote Secrecy on DRE Systems	101

[Intentionally left blank]

5 Software Requirements

5.1 Scope

This section describes essential design and performance characteristics of the software used in voting systems, addressing both system level software, such as operating systems, and voting system application software, including firmware. The requirements of this section are intended to ensure that voting system software is reliable, robust, testable, and maintainable. The requirements in this section also support system accuracy, logical correctness, privacy, security and integrity.

The general requirements of this section apply to software used to support the entire range of voting system activities described in Section 2. More specific requirements are defined for ballot counting, vote processing, creating an audit trail, and generating output reports and files. Although this section emphasizes software, the guidelines described also influence hardware design considerations.

This section recognizes that there is no best way to design software. Many programming languages are available for which modern programming practices are applicable, such as the use of rigorous program and data structures, data typing, and naming conventions. Other programming languages exist for which such practices are not easily applied.

The *Guidelines* are intended to guide the design of software written in any of the programming languages commonly used for mainframe, mini-computer, and microprocessor systems. They are not intended to preclude the use of other languages or environments, such as those that exhibit declarative structure, object-oriented languages, functional programming languages, or any other combination of language and implementation that provides appropriate levels of performance, testability, reliability, and security. The vendor makes specific software selections. However, the use of widely recognized and proven software design methods will facilitate the analysis and testing of voting system software in the certification process.

5.1.1 Software Sources

The requirements of this section apply generally to all software used in voting systems, including:

- Software provided by the voting system vendor and its component suppliers
- Software furnished by an external provider (for example, providers of COTS operating systems and web browsers) where the software may be used in any way during voting system operation
- Software developed by the voting jurisdiction

Compliance with the software requirements is assessed by several formal tests, including code examination. Unmodified software is not subject to code examination; however, source code provided by third parties and embedded in software modules for compilation or interpretation shall be provided in human readable form to the accredited test lab. The accredited test lab may inspect source code units to determine testing requirements or to verify that the code is unmodified and that the default configuration options have not been changed.

Configuration of software, both operating systems and applications, is critical to proper system functioning. Correct test design and sufficient test execution must account for the intended and proper configuration of all system components. Therefore, the vendors shall submit a record of all user selections made during software installation as part of the Technical Data Package. The vendor shall also submit a record of all configuration changes made to the software following its installation. The accredited test lab shall confirm the propriety and correctness of these user selections and configuration changes.

5.1.2 Management of Software and Hardware

The requirements of this section apply to all software used in any manner to support any voting-related activities, regardless of the ownership of the software or the ownership and location of the hardware on which the software is installed or operates. These requirements apply to:

- Software that operates on voting devices and vote counting devices installed at polling places under the control of the voting jurisdiction
- Software that operates on ballot printers, vote counting devices, and other hardware typically installed at central or precinct locations (including contractor facilities)
- Election management software

However, some requirements apply only in specific situations indicated in this section. In addition to the requirements of this section, all software used in any manner to support any voting-related activities shall meet the requirements for security described in Section 7.

5.1.3 Exclusions

Some voting systems use computers that also may be used for other purposes. General purpose software such as operating systems, programming language compilers, database management systems, and Web browsers may be installed on these computers. Such software is governed by the *Guidelines* unless:

- a. The software provides no support of voting system capabilities
- b. The software is removable, disconnectable or switchable such that it cannot function while voting system functions are enabled

- c. Procedures are provided that confirm that the software has been removed, disconnected or switched

5.2 Software Design and Coding Standards

The software used by voting systems is selected by the vendor and not prescribed by the *Guidelines*. This section provides requirements for voting system software with regard to:

- Selection of programming languages
- Software integrity
- Software modularity and programming
- Control constructs
- Naming conventions
- Coding conventions
- Comment conventions

5.2.1 Selection of Programming Languages

Software associated with the logical and numerical operations of vote data shall use a high-level programming language, such as: Pascal, Visual Basic, Java, C and C++. The requirement for the use of high-level language for logical operations does not preclude the use of assembly language for hardware-related segments, such as device controllers and handler programs. Also, operating system software may be designed in assembly language.

5.2.2 Software Integrity

Self-modifying, dynamically loaded or interpreted code is prohibited, except under the security provisions outlined in Subsection 7.4. This prohibition is to ensure that the software tested and approved during the certification process remains unchanged and retains its integrity. External modification of code during execution shall be prohibited. Where the development environment (programming language and development tools) includes the following features, the software shall provide controls to prevent accidental or deliberate attempts to replace executable code:

- a. Unbounded arrays or strings (includes buffers used to move data)
- b. Pointer variables
- c. Dynamic memory allocation and management

5.2.3 Software Modularity and Programming

Voting system application software, including commercial off-the-shelf (COTS) software, shall be designed in a modular fashion. However, COTS software is not required to be inspected for compliance with this requirement. For the purpose of this requirement¹, “modules” may be compiled or interpreted independently. Modules may also be nested. The modularity rules described here apply to the component sub-modules of a library. The principle to be followed is that the module contains all the elements to compile or interpret successfully and has limited access to data in other modules. The design concept is simple replacement with another module whose interfaces match the original module. A module is designed in accordance with the rules below.

- a. Each module shall have a specific function that can be tested and verified independently of the remainder of the code. In practice, some additional modules (such as library modules) may be needed to compile the module under test, but the modular construction allows the supporting modules to be replaced by special test versions that support test objectives.
- b. Each module shall be uniquely and mnemonically named, using names that differ by more than a single character. In addition to the unique name, the modules shall include a set of header comments identifying the module’s purpose, design, conditions, and version history, followed by the operational code. Headers are optional for modules of fewer than ten executable lines where the subject module is embedded in a larger module that has a header containing the header information. Library modules shall also have a header comment describing the purpose of the library and version information.
- c. All required resources, such as data accessed by the module, should either be contained within the module or explicitly identified as input or output to the module. Within the constraints of the programming language, such resources shall be placed at the lowest level where shared access is needed. If that shared access level is across multiple modules, the definitions should be defined in a single file (called header files in some languages, such as C) where any changes can be applied once and the change automatically applies to all modules upon compilation or activation.
- d. A module is small enough to be easy to follow and understand. Program logic visible on a single page is easy to follow and correct. Volume II, Section 5 provides testing guidelines for the accredited test lab to identify large modules subject to review under this requirement.
- e. Each module shall have a single entry point, and a single exit point, for normal process flow. For library modules or languages such as the object-oriented languages, the entry point is to the individual contained module or method invoked. The single exit point is the point where control is returned. At that point, the data that

¹ Some software languages and development environments use a different definition of module but this principle still applies.

- is expected as output must be appropriately set. The exception for the exit point is where a problem is so severe that execution cannot be resumed. In this case, the design must explicitly protect all recorded votes and audit log information and must implement formal exception handlers provided by the language.
- f. Process flow within the modules shall be restricted to combinations of the control structures defined in Volume II, Section 5. These structures support the modular concept, especially the single entry and exit rule above. They apply to any language feature where program control passes from one activity to the next, such as control scripts, object methods or sets of executable statements, even though the language itself is not procedural

5.2.4 Control Constructs

Voting system software shall use the control constructs identified in Volume II, Section 5:

- a. Acceptable constructs are Sequence, If-Then-Else, Do-While, Do-Until, Case, and the General Loop (including the special case for loop).
- i. If the programming language used does not provide these control constructs, the vendor shall provide comparable control structure logic. The constructs shall be used consistently throughout the code. No other constructs shall be used to control program logic and execution.
- ii. While some programming languages do not create programs as linear processes, stepping from an initial condition through changes to a conclusion, the program components nonetheless contain procedures (such as “methods” in object-oriented languages). Even in these programming languages, the procedures must execute through these control constructs or their equivalents, as defined and provided by the vendor.
- iii. Operator intervention or logic that evaluates received or stored data shall not re-direct program control within a program routine. Program control may be re-directed within a routine by calling subroutines, procedures, and functions, and by interrupt service routines and exception handlers (due to abnormal error conditions). Do-While (False) constructs and intentional exceptions (used as GoTos) are prohibited.

5.2.5 Naming Conventions

Voting system software shall use the naming conventions below.

- a. Object, function, procedure, and variable names shall be chosen to enhance the readability and intelligibility of the program. Insofar as possible, names shall be

selected so that their parts of speech represent their use, such as nouns to represent objects and verbs to represent functions.

- b. Names used in code and in documentation shall be consistent.
- c. Names shall be unique within an application. Names shall differ by more than a single character. All single-character names are forbidden except those for variables used as loop indexes. In large systems where subsystems tend to be developed independently, duplicate names may be used where the scope of the name is unique within the application. Names should always be unique where modules are shared.
- d. Language keywords shall not be used as names of objects, functions, procedures, variables or in any manner not consistent with the design of the language.

5.2.6 Coding Conventions

Voting system software shall adhere to basic coding conventions. The coding conventions used shall meet one of the following conditions:

- a. The vendors shall identify the published, reviewed, and industry-accepted coding conventions used and the accredited test lab shall test for compliance
- b. The accredited test lab shall evaluate the code using the coding convention requirements specified in Volume II, Section 5

These guidelines reference conventions that protect the integrity and security of the code, which may be language-specific and language-independent conventions that significantly contribute to readability and maintainability. Specific style conventions that support economical testing are not binding unless adopted by the vendor.

5.2.7 Comment Conventions

Voting system software shall use the following comment conventions:

- a. All modules shall contain headers. For small modules of 10 lines or less, the header may be limited to identification of unit and revision information. Other header information should be included in the small unit headers if not clear from the actual lines of code. Header comments shall provide the following information:
 - i. The purpose of the unit and how it works
 - ii. Other units called and the calling sequence
 - iii. A description of input parameters and outputs

- iv. File references by name and method of access (i.e., read, write, modify or append)
 - v. Global variables used
 - vi. Date of creation and a revision record
- b. Descriptive comments shall be provided to identify objects and data types. All variables shall have comments at the point of declaration clearly explaining their use. Where multiple variables that share the same meaning are required, the variables may share the same comment
- c. In-line comments shall be provided to facilitate interpretation of functional operations, tests, and branching
- d. Assembly code shall contain descriptive and informative comments such that its executable lines can be clearly understood
- e. All comments shall be formatted in a uniform manner that makes it easy to distinguish them from executable code

5.3 Data and Document Retention

All systems shall:

- a. Maintain the integrity of voting and audit data during an election, and for at least 22 months thereafter, a time sufficient to resolve most contested elections and support other activities related to the reconstruction and investigation of a contested election
- b. Protect against the failure of any data input or storage device at a location controlled by the jurisdiction or its contractors, and against any attempt at improper data entry or retrieval

5.4 Audit Record Data

Audit trails are essential to ensure the integrity of a voting system. Operational requirements for audit trails are described in Subsection 2.5.1.1. Audit record data are generated by these procedures. The audit record data in the following subsections are essential to the complete recording of election operations and reporting of the vote tally. This list of audit records may not reflect the design constructs of some systems. Therefore, vendors shall supplement it with information relevant to the operation of their specific systems.

5.4.1 Pre-election Audit Records

During election definition and ballot preparation, the system shall audit the preparation of the baseline ballot formats and modifications to them, a description of these modifications, and corresponding dates.

The log shall include:

- a. The allowable number of selections a contest
- b. The combinations of voting patterns permitted or required by the jurisdiction
- c. The inclusion or exclusion of contests as the result of multiple districting within the polling place
- d. Any other characteristics that may be peculiar to the jurisdiction, the election or the polling place location
- e. Manual data maintained by election personnel
- f. Samples of all final ballot formats
- g. Ballot preparation edit listings

5.4.2 System Readiness Audit Records

The following minimum requirements apply to system readiness audit records:

- a. Prior to the start of ballot counting, a system process shall verify hardware and software status and generate a readiness audit record. This record shall include the identification of the software release, the identification of the election to be processed, and the results of software and hardware diagnostic tests
- b. In the case of systems used at the polling place, the record shall include polling place identification
- c. The ballot interpretation logic shall test and record the correct installation of ballot formats on voting devices
- d. The software shall check and record the status of all data paths and memory locations to be used in vote recording to protect against contamination of voting data
- e. Upon the conclusion of the tests, the software shall provide evidence in the audit record that the test data have been expunged

- f. If required and provided, the ballot reader and arithmetic-logic unit shall be evaluated for accuracy, and the system shall record the results. It shall allow the processing or simulated processing of sufficient test ballots to provide a statistical estimate of processing accuracy
- g. For systems that use a public network, provide a report of test ballots that includes:
 - i. Number of ballots sent
 - ii. When each ballot was sent
 - iii. Machine from which each ballot was sent
 - iv. Specific votes or selections contained in the ballot

5.4.3 In-process Audit Records

In-process audit records document system operations during diagnostic routines and the casting and tallying of ballots. At a minimum, the in-process audit records shall contain:

- a. Machine generated error and exception messages to demonstrate successful recovery. Examples include, but are not necessarily limited to:
 - i. The source and disposition of system interrupts resulting in entry into exception handling routines
 - ii. All messages generated by exception handlers
 - iii. The identification code and number of occurrences for each hardware and software error or failure
 - iv. Notification of system login or access errors, file access errors, and physical violations of security as they occur, and a summary record of these events after processing
 - v. Other exception events such as power failures, failure of critical hardware components, data transmission errors or other types of operating anomalies
- b. Critical system status messages other than informational messages displayed by the system during the course of normal operations. These items include, but are not limited to:
 - i. Diagnostic and status messages upon startup
 - ii. The “zero totals” check conducted before opening the polling place or counting a precinct centrally

- iii. For paper-based systems, the initiation or termination of card reader and communications equipment operation
- iv. For DRE machines at controlled voting locations, the event (and time, if available) of activating and casting each ballot (i.e., each voter's transaction as an event). This data can be compared with the public counter for reconciliation purposes
- c. Non-critical status messages that are generated by the machine's data quality monitor or by software and hardware condition monitors
- d. System generated log of all normal process activity and system events that require operator intervention, so that each operator access can be monitored and access sequence can be constructed

5.4.4 Vote Tally Data

In addition to the audit requirements described above, other election-related data is essential for reporting results to interested parties, the press, and the voting public, and is vital to verifying an accurate count.

Voting systems shall meet these reporting requirements by providing software capable of obtaining data concerning various aspects of vote counting and producing printed reports. At a minimum, vote tally data shall include:

- a. Number of ballots cast, using each ballot configuration, by tabulator, by precinct, and by political subdivision
- b. Candidate and measure vote totals for each contest, by tabulator
- c. The number of ballots read within each precinct and for additional jurisdictional levels, by configuration, including separate totals for each party in primary elections
- d. Separate accumulation of overvotes and undervotes for each contest, by tabulator, precinct and for additional jurisdictional levels (no overvotes would be indicated for DRE voting devices)
- e. For paper-based systems only, the total number of ballots both able to be processed and unable to be processed; and if there are multiple card ballots, the total number of cards read

For systems that produce an electronic file containing vote tally data, the contents of the file shall include the same minimum data cited above for printed vote tally reports.

5.5 Vote Secrecy on DRE Systems

All DRE systems shall ensure vote secrecy by:

- a. Immediately after the voter chooses to cast his or her ballot, record the voter's selections in the memory to be used for vote counting and audit data (including ballot images), and erase the selections from the display, memory, and all other storage, including all forms of temporary storage
- b. Immediately after the voter chooses to cancel his or her ballot, erase the selections from the display and all other storage, including buffers and other temporary storage

[Intentionally left blank]

6 Telecommunications Requirements

Table of Contents

6	Telecommunications Requirements.....	105
6.1	Scope	105
6.1.1	Types of Components.....	106
6.1.2	Telecommunications Operations and Providers.....	106
6.1.3	Data Transmission.....	107
6.2	Design, Construction, and Maintenance Requirements	108
6.2.1	Accuracy.....	108
6.2.2	Durability.....	108
6.2.3	Reliability	108
6.2.4	Maintainability	108
6.2.5	Availability	108
6.2.6	Integrity	108
6.2.7	Confirmation.....	109

[Intentionally left blank]

6 Telecommunications Requirements

6.1 Scope

This section contains the performance, design, and maintenance characteristics of the telecommunications components of voting systems and the acceptable levels of performance against these characteristics. For the purpose of the *Guidelines*, telecommunications is defined as the capability to transmit and receive data electronically using hardware and software components over distances both within and external to a polling place.

The requirements in this section represent acceptable levels of combined telecommunications hardware and software function and performance for the transmission of data that is used to operate the system and report election results. Where applicable, this section specifies minimum values for critical performance and functional attributes involving telecommunications hardware and software components.

This section does not apply to other means of moving data, such as the physical transport of data recorded on paper-based media or the transport of physical devices, such as memory cards, that store data in electronic form.

Voting systems may include network hardware and software to transfer data among systems. Major network components are local area networks (LANs), wide area networks (WANs), workstations (desktop computers), servers, data, and applications. Workstations include voting stations, precinct tabulation systems, and voting supervisory terminals. Servers include systems that provide registration forms and ballots and accumulate and process voter registrations and cast ballots.

Desirable network characteristics include simplicity, flexibility (especially in routing, to maintain good response times) and maintainability (including availability, provided primarily through redundancy of resources and connections, particularly of connections to public infrastructure).

A wide area network (WAN) public telecommunications component consists of the hardware and software to transport information, over shared public (i.e., commercial or governmental) circuitry or among private systems. For voting systems, the telecommunications boundaries are defined as the transport circuitry, on one side of which exists the public telecommunications infrastructure, outside the control of voting system supervisors. On the other side of the transport circuitry are the local area network (LAN) resources, workstations, servers, data and applications controlled by voting system supervisors.

Local area network (LAN) components consist of the hardware and software infrastructure used to transport information between users in a local environment, typically a building or group of buildings. Typically a LAN connects workstations with a local server.

An application may be a single program or a group of programs that work together to provide a function to an end user, who may be a voter or an election administrator. Voter programs may include voter registration, balloting, and status checking. Administrator programs may include ballot preparation, registration for preparation, registration approval, ballot vetting, ballot processing, and election processing.

This section is intended to complement the network security requirements found in Section 7, which include requirements for voter and administrator access, availability of network service, data confidentiality, and data integrity. Most importantly, security services must restrict access to local election system components from public resources, and these services must also restrict access to voting system data while it is in transit through public networks.

6.1.1 Types of Components

This section addresses telecommunications hardware and software across a broad range of technologies including, but not limited to:

- Dial-up communications technologies including standard landline, wireless, microwave, Very Small Aperture Terminal, Integrated Services Digital Network, Digital Subscriber Line
- Public and private high-speed telecommunications lines including FT-1, T-1, T-3; frame relay; private line
- Cabling technologies including Universal Twisted Pair cable (CAT 5 or higher) or Ethernet hub/switch
- Wireless including radio frequency and infrared
- Communications routers
- Modems, whether internal and external to personal computers, servers, and other voting system components installed at the polling place or central count location
- Modem drivers, dial-up networking software
- Channel service units and Data service units installed at the polling place or central count location
- Dial-up networking applications software

6.1.2 Telecommunications Operations and Providers

This section applies to voting-related transmissions over public networks, such as those provided by local distribution and long distance carriers. This section also applies to private networks regardless of whether the network is owned and operated by the election jurisdiction.

For systems that transmit official data over public networks, this section applies to telecommunications components installed and operated at locations supervised by election officials, such as polling places or central offices. This includes:

- Components acquired by the jurisdiction for the purpose of voting, including components installed at the polling place or a central office (including central site facilities operated by vendors or contractors)
- Components acquired by others (such as school systems, libraries, military installations and other public organizations) that are used at locations supervised by election officials, including minimum configuration components required by the vendor but that the vendor permits to be acquired from third party sources not under the vendor's control (e.g., router or modem card manufacturer or supplier)

6.1.3 Data Transmission

These requirements apply to the use of telecommunications to transmit data for the preparation of the system for an election, the execution of an election, and the preservation of the system data and audit trails during and following an election. While this section does not assume a specific model of voting system operations and does not assume a specific model for the use of telecommunications to support such operations, it does address the following types of data, where applicable:

Voter Authentication: Coded information that confirms the identity of a voter for security purposes for a system that transmits votes individually over a public network

Ballot Definition: Information that describes to a voting machine the content and appearance of the ballots to be used in an election

Vote Transmission: For systems that transmit votes individually over a public network, the transmission of a single vote within a network at a polling place and to the county (or contractor) for consolidation with other county vote data

Vote Count: Information representing the tabulation of votes at any level within the control of the jurisdiction, such as the polling place, precinct or central count

List of Voters: A listing of the individual voters who have cast ballots in a specific election

Additional data transmissions used to operate a voting system in the conduct of an election, but not explicitly listed above, are also subject to the requirements of this section.

For systems that transmit data using public networks, this section applies to telecommunications hardware and software for transmissions within and among all combinations of senders and receivers located at polling places, precinct count facilities and central count facilities (whether operated by the jurisdiction or a contractor).

6.2 Design, Construction, and Maintenance Requirements

Design, construction, and maintenance requirements for telecommunications represent the operational capability of both system hardware and software. These capabilities shall be considered basic to all data transmissions.

6.2.1 Accuracy

The telecommunications components of all voting systems shall meet the accuracy requirements of Subsection 4.1.1.

6.2.2 Durability

The telecommunications components of all voting systems shall meet the durability requirements of Subsection 4.3.2.

6.2.3 Reliability

The telecommunications components of all voting systems shall meet the reliability requirements of Subsection 4.3.3.

6.2.4 Maintainability

The telecommunications components of all voting systems shall meet the maintainability requirements of Subsection 4.3.4.

6.2.5 Availability

The telecommunications components of all voting systems shall meet the availability requirements of Subsection 4.3.5.

6.2.6 Integrity

For WANs using public telecommunications, boundary definition and implementation shall meet the requirements below.

- a. Outside service providers and subscribers of such providers shall not be given direct access or control of any resource inside the boundary.
- b. Voting system administrators shall not require any type of control of resources outside this boundary. Typically, an end point of a telecommunications circuit will

- be a subscriber termination on a Digital Service Unit/Customer Service Unit although the specific technology configuration may vary. Regardless of the technology used, the boundary point must ensure that everything on the voting system side is locally configured and controlled by the election jurisdiction while everything on the public network side is controlled by an outside service provider.
- c. The system shall be designed and configured such that it is not vulnerable to a single point of failure in the connection to the public network which could cause total loss of voting capabilities at any polling place.

6.2.7 Confirmation

Confirmation occurs when the system notifies the user of the successful or unsuccessful completion of the data transmission, where successful completion is defined as accurate receipt of the transmitted data. To provide confirmation, the telecommunications components of a voting system shall notify the user of the successful or unsuccessful completion of the data transmission. In the event of unsuccessful transmission the user shall be notified of the action to be taken.

[Intentionally left blank]

7 Security Requirements

Table of Contents

7	Security Requirements	113
7.1	Scope	113
7.1.1	Elements of Security Outside Vendor Control	114
7.1.2	Organization of This Section	115
7.2	Access Control	115
7.2.1	General Access Control Policy	116
7.2.1.1	Individual Access Privileges	116
7.2.1.2	Access Control Measures	117
7.3	Physical Security Measures	117
7.3.1	Polling Place Security	117
7.3.2	Central Count Location Security	118
7.4	Software Security	118
7.4.1	Software and Firmware Installation	118
7.4.2	Protection Against Malicious Software	118
7.4.3	Software Distribution and Setup Validation	119
7.4.4	Software Distribution	119
7.4.5	Software Reference Information	121
7.4.5.1	Hashes and Digital Signatures	122
7.4.6	Software Setup Validation	123
7.5	Telecommunications and Data Transmission	124
7.5.1	Maintaining Data Integrity	124
7.5.2	Protection Against External Threats	125
7.5.3	Monitoring and Responding to External Threats	125
7.5.4	Shared Operating Environment	126
7.5.5	Incomplete Election Returns	127
7.6	Use of Public Communications Networks	127
7.6.1	Data Transmission	127
7.6.2	Casting Individual Ballots	128
7.6.2.1	Documentation of Mandatory Security Activities	128
7.6.2.2	Ability to Operate During Interruption of Service	128
7.7	Wireless Communications	129
7.7.1	Controlling Usage	130
7.7.2	Identifying Usage	131
7.7.3	Protecting Transmitted Data	132
7.7.4	Protecting the Wireless Path	132
7.7.5	Protecting the Voting System	133
7.8	Independent Verification Systems	134
7.8.1	Overview	134
7.8.2	Basic Characteristics of IV Systems	135
7.9	Voter Verifiable Paper Audit Trail Requirements	137
7.9.1	Display and Print a Paper Record	137

7.9.2	Approve or Void the Paper Record	137
7.9.3	Electronic and Paper Record Structure.....	138
7.9.4	Equipment Security and Reliability.....	141
7.9.5	Preserving Voter Privacy.....	142
7.9.6	VVPAT Usability	143
7.9.7	VVPAT Accessibility	144

7 Security Requirements

7.1 Scope

This section describes essential security capabilities for a voting system, encompassing the system's hardware, software, communications and documentation. No predefined set of security standards will address and defeat all conceivable or theoretical threats. The *Guidelines* articulate requirements to achieve acceptable levels of integrity and reliability. The objectives of the security standards for voting systems are:

- To protect critical elements of the voting system
- To establish and maintain controls to minimize errors
- To protect the system from intentional manipulation, fraud and malicious mischief
- To identify fraudulent or erroneous changes to the voting system
- To protect secrecy in the voting process

The *Voting System Performance Guidelines* (Volume I of the *VVSG*) are intended to address a broad range of risks to the integrity of a voting system. While it is not possible to identify all potential risks, Volume I identifies several types of risks that must be addressed. These include:

- Unauthorized changes to system capabilities for:
 - ◆ Defining ballot formats
 - ◆ Casting and recording votes
 - ◆ Calculating vote totals consistent with defined ballot formats
 - ◆ Reporting vote totals
- Alteration of voting system audit trails
- Changing, or preventing the recording of, a vote
- Introducing data for a vote not cast by a registered voter
- Changing calculated vote totals
- Preventing access to vote data—including individual votes and vote totals--by unauthorized individuals
- Preventing access to voter identification data and data for votes cast by the voter such that an individual can determine the content of specific votes

This section describes specific capabilities that vendors shall integrate into a voting system to address the risks above. Several new elements have been added since the 2002 *Voting Systems Standards*:

- Requirements for software distribution to purchasing jurisdictions
- Generation of reference information to validate software
- Validation of software using the reference information

- Requirements regarding the use of wireless communications
- Requirements for DREs with voter verifiable paper trail components

The requirements apply to the broad range of hardware, software, communications components, and documentation that comprises a voting system. These requirements apply to those components that are:

- Provided by the voting system vendor and the vendor's suppliers
- Furnished by an external provider (i.e., providers of personal computers and COTS operating systems) where the components are capable of being used during voting system operation
- Developed by a voting jurisdiction

The requirements apply to all software used in any manner to support any voting-related activity, regardless of the ownership of the software or the ownership and location of the hardware on which the software is installed or operated. These requirements apply to software that operates on:

- Voting devices and vote counting devices installed at polling places under the control or authority of the voting jurisdiction
- Ballot printers, vote counting devices, and other hardware typically installed at central or precinct locations (including contractor facilities)

7.1.1 Elements of Security Outside Vendor Control

The requirements of this section apply to the capabilities of a voting system that must be provided by the vendor. However, an effective security program requires well-defined security practices by the purchasing jurisdiction and the personnel managing and operating the system. These practices include:

- Administrative and management controls for the voting system and election management--including access controls
- Internal security procedures
- Adherence to, and enforcement of, operational procedures (e.g., effective password management)
- Security of physical facilities
- Organizational responsibilities and personnel screening

Because implementation of these elements is not under the control of the vendor, they will be addressed in the forthcoming Management Guidelines that will address the procedural aspects of conducting elections and managing the operation of voting systems. However, vendors must provide appropriate system capabilities to enable the implementation of management controls.

7.1.2 Organization of This Section

The guidelines presented in this section are organized as follows:

Access Control: These standards address procedures and system capabilities that limit or detect access to critical system components in order to guard against loss of system integrity, availability, confidentiality, and accountability.

Physical Security: These standards address physical security measures and procedures that prevent disruption of the voting process at the polling place and corruption of voting data.

Software Security: These standards address the installation of software, including firmware, in the voting system and the protection against malicious software. It should be noted that computer-generated audit controls facilitate system security and are an integral part of software capability. These audit requirements are presented in Subsection 5.4.

Telecommunications and Data Transmission: These standards address security for the electronic transmission of data between system components or locations over private, public, and wireless networks.

Use of Public Communications Networks: These standards address security for systems that communicate individual votes or vote totals over public communications networks.

Wireless Communications: These standards address the security of the voting system and voting data when wireless is used.

Independent Verification Systems: This section provides an introduction to the concept of independent verification as a method to demonstrate voting system integrity. This discussion provides the context for the requirements for DREs with voter verifiable paper audit trails.

Direct-Recording Electronic Systems with Voter Verifiable Paper Audit Trails (optional): This capability is not required for national certification. These guidelines are provided for use by states that require this feature for DRE systems.

7.2 Access Control

Access controls are procedures and system capabilities that detect or limit access to system components in order to guard against loss of system integrity, availability, confidentiality, and accountability. Access controls provide reasonable assurance that system resources such as data files, application programs, and computer-related facilities and equipment are protected against unauthorized operation, modification, disclosure, loss or impairment. Unauthorized operations include modification of compiled or interpreted code, run-time

alteration of flow control logic or of data, and abstraction of raw or processed voting data in any form other than a standard output report by an authorized operator.

Access controls may include physical controls, such as keeping computers in locked rooms to limit physical access, and technical controls, such as security software programs designed to prevent or detect unauthorized access to sensitive files. The access controls described in this section are limited to those controls required to be provided by system vendors.

7.2.1 General Access Control Policy

The vendor shall specify the general features and capabilities of the access control policy recommended to provide effective voting system security.

Although the jurisdiction in which the voting system is operated is responsible for determining the access policies for each election, the vendor shall provide a description of recommended policies for:

- a. Software access controls
- b. Hardware access controls
- c. Communications
- d. Effective password management
- e. Protection abilities of a particular operating system
- f. General characteristics of supervisory access privileges
- g. Segregation of duties
- h. Any additional relevant characteristics

7.2.1.1 Individual Access Privileges

Voting system vendors shall:

- a. Identify each person to whom access is granted, and the specific functions and data to which each person holds authorized access
- b. Specify whether an individual's authorization is limited to a specific time, time interval or phase of the voting or counting operations
- c. Permit the voter to cast a ballot expeditiously, but preclude voter access to all aspects of the vote counting processes

7.2.1.2 Access Control Measures

Vendors shall provide a detailed description of all system access control measures designed to permit authorized access to the system and prevent unauthorized access. Examples of such measures include:

- a. Use of data and user authorization
- b. Program unit ownership and other regional boundaries
- c. One-end or two-end port protection devices
- d. Security kernels
- e. Computer-generated password keys
- f. Special protocols
- g. Message encryption
- h. Controlled access security

Vendors also shall define and provide a detailed description of the methods used to prevent unauthorized access to the access control capabilities of the system itself.

7.3 Physical Security Measures

A voting system's sensitivity to disruption or corruption of data depends, in part, on the physical location of equipment and data media, and on the establishment of secure telecommunications among various locations. Most often, the disruption of voting and vote counting results from a physical violation of one or more areas of the system thought to be protected. Therefore, security procedures shall address physical threats and the corresponding means to defeat them.

7.3.1 Polling Place Security

For polling place operations, vendors shall develop and provide detailed documentation of measures to enable poll workers to physically protect and perform orderly shutdown of voting equipment to counteract vandalism, civil disobedience, and similar occurrences.

The measures shall allow the immediate detection of tampering with vote casting devices and precinct ballot counters. They also shall control physical access to a telecommunications link if such a link is used

7.3.2 Central Count Location Security

Vendors shall develop and document in detail the measures to be taken in a central counting environment. These measures shall include physical and procedural controls related to the handling of ballot boxes, preparing of ballots for counting, counting operations and reporting data.

7.4 Software Security

Voting systems shall meet specific security requirements for the installation of software and for protection against malicious software.

7.4.1 Software and Firmware Installation

The system shall meet the following requirements for installation of software, including hardware with embedded firmware.

- a. If software is resident in the system as firmware, the vendor shall require and state in the system documentation that every device is to be retested to validate each ROM prior to the start of elections operations.
- b. To prevent alteration of executable code, no software shall be permanently installed or resident in the voting system unless the system documentation states that the jurisdiction must provide a secure physical and procedural environment for the storage, handling, preparation, and transportation of the system hardware.
- c. The voting system bootstrap, monitor, and device-controller software may be resident permanently as firmware, provided that this firmware has been shown to be inaccessible to activation or control by any means other than by the authorized initiation and execution of the vote counting program, and its associated exception handlers.
- d. The election-specific programming may be installed and resident as firmware, provided that such firmware is installed on a component (such as a computer chip) other than the component on which the operating system resides.
- e. After initiation of election day testing, no source code or compilers or assemblers shall be resident or accessible.

7.4.2 Protection Against Malicious Software

Voting systems shall deploy protection against the many forms of threats to which they may be exposed such as file and macro viruses, worms, Trojan horses, and logic bombs. Vendors

shall develop and document the procedures to be followed to ensure that such protection is maintained in a current status.

7.4.3 Software Distribution and Setup Validation

Subsections 7.4.4, 7.4.5 and 7.4.6 specify requirements for the distribution of voting system software and the setup validation performed on voting system equipment. These requirements are applicable to voting systems that have completed certification testing. The goal of the software distribution requirements is to ensure that the correct voting system software has been distributed without modification. The goal of setup validation requirements, including requirements for verifying the presence of certified software and the absence of other software, is to ensure that voting system equipment is in a proper initial state before being used.

In general, a voting system can be considered to be composed of multiple associated systems including polling place systems, central counting/aggregation systems, and election management systems. These other systems may reside on different computer platforms at different locations and run different software. Voting system software is considered to be all executable code and associated configuration files critical for the proper operation of the voting system regardless of the location of installation and functionality provided. This includes third party software such as operating systems, drivers, and database management systems.

7.4.4 Software Distribution

- a. The vendor shall document all software including voting system software, third party software (such as operating systems and drivers) to be installed on the certified voting system, and installation programs.
 - i. The documentation shall have a unique identifier (such as a serial number or part number) for the following set of information: documentation, software vendor name, product name, version, the certification application number of the voting system, file names and paths or other location information (such as storage addresses) of the software.
 - ii. The documentation shall designate all software files as static, semi-static or dynamic.

Discussion: Static voting system software such as executable code does not change based on the election being conducted or the voting equipment upon which it is installed. Semi-static voting system software contains configuration information for the voting system based on the voting equipment that is installed and the election being conducted. Semi-static software is only modified during the installation of (a) the voting system software on voting equipment or (b) the election-specific software such

as ballot formats. Dynamic voting system software changes over time once installed on voting equipment. However, the specific time or value of the change in the dynamic software is usually unknown in advance, making it impossible to create reference information to verify the software.

b. The EAC accredited testing lab shall witness the final build of the executable version of the certified voting system software performed by the vendor.

- i. The testing lab shall create a complete record of the build that includes: a unique identifier (such as a serial number) for the complete record; a list of unique identifiers of unalterable storage media associated with the record; the time, date, location, names and signatures of all people present; the source code and resulting executable file names; the version of voting system software; the certification application number of the voting system; the name and versions of all (including third party) libraries; and the name, version, and configuration files of the development environment used for the build.
- ii. The record of the source code and executable files shall be made on unalterable storage media. Each piece of media shall have a unique identifier.

Discussion: Unalterable storage media includes technology such as a CD-R, but not CD-RW. The unique identifiers appear on indelibly printed labels and in a digitally signed file on the unalterable storage media.

- iii. The testing lab shall retain this record until notified by the EAC that it can be archived.

c. After EAC certification has been granted, the testing lab shall create a subset of the complete record of the build that includes a unique identifier (such as a serial number) of the subset, the unique identifier of the complete record, a list of unique identifiers of unalterable storage media associated with the subset, the vendor and product name, the version of voting system software, the certification number of the voting system, and all the files that resulted from the build and binary images of all installation programs.

- iii. The record of the software shall be made on unalterable storage media. Each piece of media shall have a unique identifier.

- iv. The testing lab shall retain a copy, send a copy to the vendor, and send a copy to the NIST National Software Reference Library (NSRL)² and/or to any repository designated by a State.

² The National Software Reference Library (NSRL) is a repository of software maintained by the National Institute of Standards and Technology. It was designed to meet the need for court admissible evidence in the identification of software files. The EAC has designated the NSRL as a repository for voting system software. Information is available at www.nsrl.nist.gov.

- v. The NSRL shall retain this software until notified by the EAC that it can be archived.
- d. The vendor shall provide the NSRL and any repository designated by a state with a copy of the software installation disk, which the vendor will distribute to purchasers--including the executable binary images of all third party software.
 - i. All voting system software, installation programs and third party software (such as operating systems and drivers) used to install or to be installed on voting system equipment shall be distributed using unalterable storage media.
 - ii. The vendor shall document that the process used to verify the software distributed on unalterable storage media is the certified software by using the reference information provided by the NSRL or other designated repository before installing the software.
- e. The voting system equipment shall be designed to allow the voting system administrator to verify that the software is the certified software by comparing it to reference information produced by the NSRL or other designated repository.
- f. The vendors and testing labs shall document to whom they provide voting system software.

7.4.5 Software Reference Information

The NSRL or other repository designated by a state election office shall generate reference information using the binary images of the (a) certified voting system software received on unalterable storage media from testing labs and (b) election- specific software received on unalterable storage media from jurisdictions.

- a. The NSRL or other designated repository shall generate reference information in at least one of the following forms: (a) complete binary images, (b) cryptographic hash values or (c) digital signatures of the software.

Discussion: Although binary images, cryptographic hashes, and digital signatures can detect a modification or alteration in the software, they cannot determine if the change to the software was accidental or intentional.

- b. The NSRL or other designated repository shall create a record of the creation of reference information that includes: a unique identifier (such as a serial number) for the record; the file names of software and associated unique identifier(s) of the unalterable storage media from which reference information is generated; the time, date and name of people who generated reference information; the type of reference information created; the certification number of the voting system; the voting system software version; the product name; and the vendor name.

- c. The NSRL or other designated repository shall retain the unalterable storage media used to generate the reference information until notified by the EAC that it can be archived.

7.4.5.1 Hashes and Digital Signatures

- a. The NSRL or other designated repository that generates hash value and/or digital signature reference information shall use FIPS-approved algorithms for hashing and signing.

- i. The NSRL or other designated repository that generates hash values, digital signatures reference information or cryptographic keys shall use a FIPS 140-2 level 1 or higher validated cryptographic module.

Discussion: See <http://www.csrc.nist.gov/cryptval/> for information on FIPS 140-2.

- ii. The NSRL or other designated repository that generates sets of hash values and digital signatures for reference information shall include a hash value or digital signature covering the set of reference information.

- b. If the NSRL or other designated repository uses public key technology, the following requirements shall be met:

- i. Public and private key pairs used by the repository to generate digital signatures shall be 2048-bits or greater in length
 - ii. The repository's private keys used to generate digital signature reference information shall be used for no more than three years
 - iii. Public keys used to verify digital signature reference information shall be placed on unalterable storage media if not contained in a signed non-proprietary format for distribution.

Discussion: Examples of non-proprietary standard formats include X.509 or PKCS#7.

- iv. All copies of public key unalterable storage media made by the repository shall be labeled so that they are uniquely identifiable, including at a minimum: a unique identifier (such as a serial number) for the unalterable storage media; the time, date, location and name(s) of the repository owning the associated private keys; documentation about its creation; and an indication that the contents are public keys.
 - v. The NSRL or other designated repository shall document to whom they provide unalterable storage media containing their public keys used to verify digital signature reference information including at a minimum: the uniquely identified

public keys, the time and date provided, the name of the organization, and the name and contact information (phone, address, email address) of the recipient.

- vi. When a private key used to generate digital signature reference information becomes compromised, the NSRL or other designated repository shall provide notification to recipients of the associated public key that the private key has been compromised and the date on which it was compromised.
- c. The NSRL or other designated repository shall make both the reference information available on unalterable storage media and its associated documentation that is labeled by the repository that created it uniquely identifiable by including at a minimum: a unique identifier (such as a serial number) for the storage media; the time, date, location and name of the creating repository; and an indication that the contents are reference information.

7.4.6 Software Setup Validation

- a. Setup validation methods shall verify that no unauthorized software is present on the voting equipment.
- b. The vendor shall have a process to verify that the correct software is loaded, that there is no unauthorized software, and that voting system software on voting equipment has not been modified, using the reference information from the NSRL or from a State designated repository.
 - i. The process used to verify software should be possible to perform without using software installed on the voting system.
 - ii. The vendor shall document the process used to verify software on voting equipment.
 - iii. The process shall not modify the voting system software on the voting system during the verification process.
- c. The vendor shall provide a method to comprehensively list all software files that are installed on voting systems.
- d. The verification process should be able to be performed using COTS software and hardware available from sources other than the voting system vendor.
 - i. If the process uses hashes or digital signatures, then the verification software shall use a FIPS 140-2 level 1 or higher validated cryptographic module.
 - ii. The verification process shall either (a) use reference information on unalterable storage media received from the repository or (b) verify the digital signature of the reference information on any other media.

- e. Voting system equipment shall provide a means to ensure that the system software can be verified through a trusted external interface, such as a read-only external interface, or by other means.
 - i. The external interface shall be protected using tamper evident techniques
 - ii. The external interface shall have a physical indicator showing when the interface is enabled and disabled
 - iii. The external interface shall be disabled during voting
 - iv. The external interface should provide a direct read-only access to the location of the voting system software without the use of installed software
- f. Setup validation methods shall verify that registers and variables of the voting system equipment contain the proper static and initial values.
 - i. The vendor should provide a method to query the voting system to determine the values of all static and dynamic registers and variables including the values that jurisdictions are required to modify to conduct a specific election.
 - ii. The vendor shall document the values of all static registers and variables, and the initial starting values of all dynamic registers and variables listed for voting system software, except for the values set to conduct a specific election.

7.5 Telecommunications and Data Transmission

There are four areas that must be addressed by telecommunications and data transmission security capabilities: access control, data integrity, detection and prevention of data interception, and protection against external threats.

7.5.1 Maintaining Data Integrity

Voting systems that use telecommunications to communicate between system components and locations are subject to the same security requirements governing access to any other system hardware, software, and data function.

- a. Voting systems that use electrical or optical transmission of data shall ensure the receipt of valid vote records is verified at the receiving station. This should include standard transmission error detection and correction methods such as checksums or message digest hashes. Verification of correct transmission shall occur at the voting system application level and ensure that the correct data is recorded on all relevant components consolidated within the polling place prior to the voter completing casting of his or her ballot.

- b. Voting systems that use telecommunications to communicate between system components and locations before the polling place is officially closed shall:
 - i. Implement an encryption standard currently documented and validated for use by an agency of the U.S. government
 - ii. Provide a means to detect the presence of an intrusive process, such as an Intrusion Detection System

7.5.2 Protection Against External Threats

- a. Voting systems that use public telecommunications networks shall implement protections against external threats to which commercial products used in the system may be susceptible.
- b. Voting systems that use public telecommunications networks shall provide system documentation that clearly identifies all COTS hardware and software products and communications services used in the development and/or operation of the voting system, including operating systems, communications routers, modem drivers and dial-up networking software.
 - i. Such documentation shall identify the name, vendor, and version used for each such component.
- c. Voting systems that use public telecommunications networks shall use protective software at the receiving-end of all communications paths to:
 - i. Detect the presence of a threat in a transmission
 - ii. Remove the threat from infected files/data
 - iii. Prevent against storage of the threat anywhere on the receiving device
 - iv. Provide the capability to confirm that no threats are stored in system memory and in connected storage media
 - v. Provide data to the system audit log indicating the detection of a threat and the processing performed
- d. Vendors shall use multiple forms of protective software as needed to provide capabilities for the full range of products used by the voting system.

7.5.3 Monitoring and Responding to External Threats

Voting systems that use public telecommunications networks may become vulnerable, by virtue of their system components, to external threats to the accuracy and integrity of vote

recording, vote counting, and vote consolidation and reporting processes. Therefore, vendors of such systems shall document how they plan to monitor and respond to known threats to which their voting systems are vulnerable. This documentation shall provide a detailed description, including scheduling information, of the procedures the vendor will use to:

- a. Monitor threats, such as through the review of assessments, advisories, and alerts for COTS components issued by the Computer Emergency Response Team (CERT), for which a current listing can be found at <http://www.cert.org>, the National Infrastructure Protection Center (NIPC), and the Federal Computer Incident Response Capability (FedCIRC), for which additional information can be found at www.us-cert.gov
- b. Evaluate the threats and, if any, proposed responses
- c. Develop responsive updates to the system and/or corrective procedures
- d. Submit the proposed response to the test labs and appropriate states for approval, identifying the exact changes and whether or not they are temporary or permanent
- e. After implementation of the proposed response is approved by the state, assist clients, either directly or through detailed written procedures, how to update their systems and/or to implement the corrective procedures within the timeframe established by the state
- f. Address threats emerging too late to correct the system by:
 - i. Providing prompt, emergency notification to the accredited test labs and the affected states and user jurisdictions
 - ii. Assisting client jurisdictions directly or advising them through detailed written procedures to disable the public telecommunications mode of the system
 - iii. Modifying the system after the election to address the threat, submitting the modified system to an accredited test lab and the EAC or state certification authority for approval, and assisting client jurisdictions directly or advising them through detailed written procedures, to update their systems and/or to implement the corrective procedures after approval

7.5.4 Shared Operating Environment

Ballot recording and vote counting can be performed in either a dedicated or non-dedicated environment. If ballot recording and vote counting operations are performed in an environment that is shared with other data processing functions, both hardware and software features shall be present to protect the integrity of vote counting and of vote data.

Systems that use a shared operating environment shall:

- a. Use security procedures and logging records to control access to system functions
- b. Partition or compartmentalize voting system functions from other concurrent functions at least logically, and preferably physically as well
- c. Control system access by means of passwords, and restrict account access to necessary functions only
- d. Have capabilities in place to control the flow of information, precluding data leakage through shared system resources

7.5.5 Incomplete Election Returns

If the voting system provides access to incomplete election returns and interactive inquiries before the completion of the official count, the system shall:

- a. Be designed to provide external access to incomplete election returns (for equipment that operates in a central counting environment), only if that access for these purposes is authorized by the statutes and regulations of the using agency. This requirement applies as well to polling place equipment that contains a removable memory module or that may be removed in its entirety to a central place for the consolidation of polling place returns
- b. Design voting system software and its security environment such that data accessible to interactive queries resides in an external file or database created and maintained by the elections software under the restrictions applying to any other output report:
 - i. The output file or database has no provision for write access back to the system
 - ii. Persons whose only authorized access is to the file or database are denied write access, both to the file or database, and to the system

7.6 Use of Public Communications Networks

Voting systems that transmit data over public telecommunications networks face security risks that are not present in other voting systems. This section describes standards applicable to voting systems that use public telecommunications networks.

7.6.1 Data Transmission

All systems that transmit data over public telecommunications networks shall:

- a. Preserve the secrecy of voter ballot selections and prevent anyone from violating ballot privacy

- b. Employ digital signatures for all communications between the vote server and other devices that communicate with the server over the network
- c. Require that at least two authorized election officials activate any critical operation regarding the processing of ballots transmitted over a public communications network, i.e. the passwords or cryptographic keys of at least two employees are required to perform processing of votes

7.6.2 Casting Individual Ballots

Systems designed for transmission of telecommunications over public networks shall meet security standards that address the security risks attendant with the casting of ballots from polling places controlled by election officials using voting devices configured and installed by election officials and/or their vendor or contractor, and using in-person authentication of individual voters.

7.6.2.1 Documentation of Mandatory Security Activities

Vendors of voting systems that cast individual ballots over a public telecommunications network shall provide detailed descriptions of:

- a. All activities mandatory to ensuring effective voting system security to be performed in setting up the system for operation, including testing of security before an election
- b. All activities that should be prohibited during voting equipment setup and during the timeframe for voting operations, including both the hours when polls are open and when polls are closed

7.6.2.2 Ability to Operate During Interruption of Service

These systems shall provide the following capabilities to provide resistance to interruptions of telecommunications service that prevent voting devices at the polling place from communicating with external components via telecommunications:

- a. Detect the occurrence of a telecommunications interruption at the polling place and switch to an alternative mode of operation that is not dependent on the connection between polling place voting devices and external system components
- b. Provide an alternate mode of operation that includes the functionality of a conventional electronic voting system without losing any single vote
- c. Create and preserve an audit trail of every vote cast during the period of interrupted communication and system operation in conventional electronic voting system mode

- d. Upon reestablishment of communications, transmit and process votes accumulated while operating in conventional electronic voting system mode with all security safeguards in effect
- e. Ensure that all safeguards related to voter identification and authentication are not affected by the procedures employed by the system to counteract potential interruptions of telecommunications capabilities

7.7 Wireless Communications

This section provides requirements for implementing and using wireless communications within a voting system. These requirements reduce, but do not eliminate, the risk of using wireless communications for voting systems.

Wireless is defined as any means of communications that occurs without wires. This normally covers the entire electromagnetic spectrum. For the purposes of this section, wireless includes radio frequency, infrared, and microwave. This section provides requirements and considerations that apply to external wireless communications capabilities existing on voting equipment or as a component within a voting system. These requirements may be applied to internal wireless communications, but this is not required when the physical container that houses the voting equipment or voting system is considered adequate to protect the internal wireless between or among voting system components.

Since the wireless communications path on which the signals travel is via the air and not a wire or cable, devices other than those intended to receive the wireless signal (e.g. voting data) can receive (intentionally and unintentionally) the wireless signals. Some of the wireless communications paths (i.e. signals) are weakened by walls and distance, but are not stopped. This makes it possible to eavesdrop from a distance as well as transmit wireless signals (e.g., interference or intrusive data) from a distance. In many cases, the wireless signals cannot be seen, heard, or felt, thus making the presence of wireless communication hard to determine by the human senses. The requirements in this section mitigate the risks associated with wireless by controlling and identifying usage, and protecting the transmitted data and path.

There are other concerns when evaluating wireless usage; specifically radio frequency (RF). A device's radio frequencies usage and the power output are governed by Federal Communications Commission (FCC) regulations and therefore all RF wireless communications devices are subject to the applicable FCC requirements. However, these FCC regulations do not fully address RF wireless interference caused by multiple FCC compliant devices. That is, the RF wireless used in a voting system may be using the same radio frequency as another non-voting wireless system and which may potentially cause a degradation of the wireless performance or a complete wireless failure for the voting system.

Sometimes a particular wireless technology permits a power output range, which may be used to overcome interference received from another device. A radio emissions site test can

determine the extent of potential existing interference at the location where the wireless voting system is to be used. A radio emission site test can also determine the extent that the RF wireless transmission of the voting system escapes the building in which the RF wireless voting system is used.

7.7.1 Controlling Usage

- a. If wireless communications are used in a voting system, then the vendor shall supply documentation describing how to use all aspects of wireless communications in a secure manner. This documentation shall include:
 - i. A complete description of the uses of wireless in the voting system including descriptions of the data elements and signals that are to be carried by the wireless mechanism
 - ii. A complete description of the vulnerabilities associated with this proposed use of wireless, including vulnerabilities deriving from the insertion, deletion, modification, capture or suppression of wireless messages
 - iii. A complete description of the techniques used to mitigate the risks associated with the described vulnerabilities including techniques used by the vendor to ensure that wireless cannot send or receive messages other than those situations specified in the documentation. Cryptographic techniques shall be carefully and fully described, including a description of cryptographic key generation, management, use, certification, and destruction
 - iv. A rationale for the inclusion of wireless in the proposed voting system, based on a careful and complete description of the perceived advantages and disadvantages of using wireless for the documented uses compared to using non-wireless approaches
- Discussion: In general, convenience is not a sufficiently compelling reason, on its own, to justify the inclusion of wireless communications in a voting system. Convenience must be balanced against the difficulty of working with cryptographic keys.
- b. The details of all cryptographic protocols used for wireless communications, including the specific features and data, shall be documented.
- c. The wireless documentation shall be closely reviewed for accuracy, completeness, and correctness.

- d. There shall be no undocumented use of the wireless capability, nor any use of the wireless capability that is not entirely controlled by an election official.

Discussion: This can be tested by reviewing all of the software, hardware, and documentation, and by testing the status of wireless activity during all phases of testing.

- e. If a voting system includes wireless capabilities, then the voting system shall be able to accomplish the same function if wireless capabilities are not available due to an error or no service.
 - i. The vendor shall provide documentation how to accomplish these functions when wireless is not available.
- f. The system shall be designed and configured so it is not vulnerable to a single point of failure using wireless communications that causes a total loss of any voting capabilities.
- g. If a voting system includes wireless capabilities, then the system shall have the ability to turn on the wireless capability when it is to be used and to turn off the wireless capability when the wireless capability is not in use.
- h. If a voting system includes wireless capabilities, then the system shall not activate the wireless capabilities without confirmation from an elections official.

7.7.2 Identifying Usage

Since there are a wide variety of wireless technologies (both standard and proprietary) and differing physical properties of wireless signals, it is important to identify some of the characteristics of the wireless technologies used in the voting system.

- a. If a voting system provides wireless communications capabilities, then there shall be a method for determining the existence of the wireless communications capabilities.
- b. If a voting system provides wireless communications capabilities, then there shall be an indication that allows one to determine when the wireless communications (such as radio frequencies) capability is active.
- c. The indication shall be visual.
- d. If a voting system provides wireless communications capabilities, then the type of wireless communications used (such as radio frequencies) shall be identified either via a label or via the voting system documentation.

7.7.3 Protecting Transmitted Data

The transmitted data, especially via wireless communications, needs to be protected to ensure confidentiality and integrity. Examples of election information that needs to be protected include: ballot definitions, voting device counts, precinct counts, opening of poll signal, and closing of poll signal. Examples of other information that needs to be protected include: protocol messages, address or device identification information, and passwords.

Since radio frequency wireless signals radiate in all directions and pass through most construction material, anyone may easily receive the wireless signals. In contrast, infrared signals are line of sight and do not pass through most construction material. However, infrared signals can still be received by other devices that are in the line of sight. Similarly, wireless signals can be transmitted by others to create unwanted signals. Thus, encryption is required to protect the privacy and confidentiality of the voting information.

- a. All information transmitted via wireless communications shall be encrypted and authenticated--with the exception of wireless T-coil coupling--to protect against eavesdropping and data manipulation including modification, insertion, and deletion.
 - i. The encryption shall be as defined in Federal Information Processing Standards (FIPS) 197, "Advanced Encryption Standard (AES)."
 - ii. The cryptographic modules used shall comply with FIPS 140-2, Security Requirements for Cryptographic Modules.
- b. The capability to transmit non-encrypted and non-authenticated information via wireless communications shall not exist.
- c. If audible wireless communication is used, and the receiver of the wireless transmission is the human ear, then the information shall not be encrypted.

Discussion: This specifically covers wireless T-Coil coupling for assistive devices used by people who are hard of hearing.

7.7.4 Protecting the Wireless Path

If wireless communications are used, then the following capabilities shall exist in order to mitigate the effects of a denial of service (DoS) attack:

- a. The voting system shall be able to function properly throughout a DoS attack, since the DoS attack may continue throughout the voting period.
- b. The voting system shall function properly as if the wireless capability were never available for use.
- c. Alternative procedures or capabilities shall exist to accomplish the same functions that the wireless communications capability would have done.
- d. If infrared is being used, the shielding shall be strong enough to prevent escape of the voting system signal, as well as strong enough to prevent infrared saturation jamming.

Discussion: Since infrared has the line-of-sight property, securing the wireless path can be accomplished by shielding the path between the communicating devices with an opaque enclosure. However, this is only practical for short distances. This shielding would also help prevent accidental eye damage from the infrared signal.

7.7.5 Protecting the Voting System

Physical security measures to prevent access to a voting system are not possible when using a wireless communications interface because there is no discrete physical communications path that can be secured.

- a. The security requirements in Subsection 2.1.1 shall be applicable to systems with wireless communications.
- b. The accuracy requirements in Subsection 2.1.2 shall be applicable to systems with wireless communications.
- c. The use of wireless communications that may cause impact to the system accuracy through electromagnetic stresses is prohibited.
- d. The error recovery requirements in Subsection 2.1.3 shall be applicable to systems with wireless communications.
- e. All wireless communications actions shall be logged.
 - i. The log shall contain at least the following entries: times when the wireless is activated and deactivated, services accessed, identification of device to which data was transmitted to or received from, identification of authorized user, and successful and unsuccessful attempts to access wireless communications or service.

Discussion: Other information such as the number of frames or packets transmitted or received at various logical layers may be useful, but is dependent on the wireless technology used.

- f. Device authentication shall occur before any access to, or services from, the voting system are granted through wireless communications.

Discussion: Authentication is an important element to protect the security of wireless communications. Authentication verifies the identity and legitimacy of users, devices, and services.

- i. User authentication shall be at least level 2 as per NIST Special Publication 800-63 Version 1.0.1, Electronic Authentication Guideline.

7.8 Independent Verification Systems

7.8.1 Overview

Independent verification (IV) systems are electronic voting systems that produce multiple independent cast vote records of voter ballot selections, which can be audited to a high level of precision. For this to happen, the cast vote records must be handled according to the following protocol:

- At least two cast vote records of the voter's selections are produced and one of the records is then stored in a manner that it cannot be modified by the voting system. For example, the voting system creates a record of the voter's selections and then copies it to unalterable storage media.
- The voter must be able to verify that both cast vote records are correct and match before leaving the polling place, e.g., verify his or her selections on the voting machine summary screen and also verify the second record on the unalterable storage media.
- The verification processes for the two cast vote records must be independent of each other, and at least one of the records must be verified directly by the voter.
- The contents of the two cast vote records also can be checked later for consistency through the use of unique identifiers that allow the records to be linked.

The cast vote records would be formatted so that at least one set is usable in an efficient counting process by the electronic voting system and the other set is usable in an efficient process of auditing or verifying the agreement between the two sets.

Given these conditions, the multiple cast vote records are considered to be distinct and independently verifiable, that is, both records are not under the control of the same system processes. As a result of this independence, the audit records can be used to check the accuracy of the counted records. Because the records are separately stored, an attacker who can compromise one will also have to compromise the other.

The voter verifiable paper audit trail (VVPAT) methodology is one of several classes of IV systems. In this approach, the voter can directly compare the electronic summary screen of the voting machine with the printed paper audit record. (This is not to be confused with the

paper ballot that is produced by optical scan voting systems that the voter visually verifies before placing it in the ballot box or tabulator.) Requirements for DREs with a VVPAT feature are provided below to reflect the fact that a number of States currently require this feature.

There are a variety of other IV approaches for the voter to verify his or her selections with systems that produce an electronic record for verification. Appendix C describes the characteristics of these systems in more detail. They include:

- Split process systems, which use separate devices for the voters to record and verify their ballot selections
- Cryptographic systems, which provide voters with coded receipts that can be used to verify their ballot selections
- Witness systems, which use an independent module to create the second record

7.8.2 Basic Characteristics of IV Systems

This section describes a preliminary set of basic characteristics that apply to all types of IV systems. This information is provided for the purpose of introducing these concepts for consideration in voting system design. It is anticipated that future voting systems will be required to provide some type of independent verification feature to enable voters to have confidence that their ballot selections are correctly recorded and counted.

An independent verification system produces at least two independent cast vote records of ballot selections via interactions with the voter, such that one record can be compared against the other to check their equality of content.

Discussion: This is the fundamental characteristic of IV systems. The records can be checked against one another to determine whether or not the voter selections are correctly recorded.

The voter verifies the content of each cast vote record and either (a) verifies at least one of the records directly or (b) verifies both records indirectly if the records are each under the control of independent processes.

Discussion: Direct verification involves using human senses; for example, directly reading a paper record via one's eyesight. Indirect verification involves using an intermediary to perform the verification; for example, verifying an electronic ballot image on the voting machine.

The creation, storage and handling of the cast vote records are sufficiently separate that the failure or compromise of one record does not cause the failure or compromise of another.

Discussion: The records must be stored on different media and handled independently of each other so that no one process could compromise all records. If an attack can alter one record, it should still be very difficult to alter the other record.

Both cast vote records are highly resistant to damage or alteration and capable of long-term storage.

Discussion: The records should be difficult to alter or damage so that they could be used in case the counted records are damaged or lost.

The processes of verification for the cast vote records do not all depend on the same device, software module, or system for their integrity, and are sufficiently separate that each record provides evidence of the voter's selections independently of its corresponding record.

Discussion: For example, the verification of the summary screen (electronic record) of a DRE is sufficiently separate from the verification of a paper record printed by a VVPAT component or a copy of the electronic record stored on a separate system.

The multiple cast vote records are linked to their corresponding audit records by including a unique identifier within each record.

Discussion: The identifier serves the purpose of uniquely identifying and linking the records for cross-checking.

Each cast vote record includes information identifying the following:

- An identification of the polling place and precinct
- Whether the balloting is provisional, early, or on election day
- Ballot style
- A timestamp generated when the voting machine is enabled to begin a voting session that can be used to correctly group the cast vote records
- A unique identifier associated with the voting machine

Discussion: The identifier could be a serial number or other unique ID.

The cryptographic software used in IV systems is approved by the U.S. Government's Cryptographic Module Validation Program, as applicable.

Discussion: IV voting systems may use cryptographic software for a number of different purposes, including calculating checksums, encrypting records, authentication, generating random numbers, and for digital signatures. This software should be reviewed and approved by the Cryptographic Module Validation Program (CMVP). There may be cryptographic voting schemes where the cryptographic algorithms used are necessarily different from any algorithms that have approved CMVP implementations, thus CMVP-approved software shall be used where feasible. The CMVP website is <http://csrc.nist.gov/cryptval>.

7.9 Voter Verifiable Paper Audit Trail Requirements

This section contains requirements for DREs with a Voter Verifiable Paper Audit Trail (VVPAT) component. VVPAT capability is not required for national certification. However, these requirements will be applied for certification testing of DRE systems that are intended for use in states that require DREs to provide this capability. The vendor's certification testing application to the EAC must indicate whether the system being presented for testing includes this capability, as provided under Subsection 1.6.2.5 extensions.

7.9.1 Display and Print a Paper Record

- a. The voting system shall print and display a paper record of the voter ballot selections prior to the voter making his or her selections final by casting the ballot.

Discussion: This is the basic requirement for VVPAT capability. It requires the paper record to be created as a distinct representation of the voter ballot selections. It requires the paper record to contain the same information as the electronic record and be suitable for use in verifications of the voting machine's electronic records.

- b. The paper record shall constitute a complete record of ballot selections that can be used to assess the accuracy of the voting machine's electronic record, to verify the election results, and, if required by state law, in full recounts.

Discussion: This requirement exists to make clear that it is possible to use the paper record for checks of the voting machine's accuracy in recording voter ballot selections, as well as usable for election audits (such as mandatory 1% recounts). The paper record shall also be suitable for use in full recounts of the election if required by state law.

- c. The paper record shall contain all voter selection information stored in the electronic (ballot image) record.

Discussion: The electronic ballot image record cannot hide any information related to ballot selections; all information relating to voter selections must be equally present in both records. The electronic record may contain other items that don't necessarily need to be on the paper record, such as digital signature information.

7.9.2 Approve or Void the Paper Record

- a. The voting equipment shall allow the voter to approve or void the paper record.

Discussion: There are three possible scenarios regarding the voter's disposition of the paper record.

- The voter can verify that the ballot selections displayed on the DRE summary screen and those printed on the paper record are the same. If they are, and the voter is satisfied with these selections, the voter can proceed to cast his or her ballot, thereby approving the paper record.
 - If the selections match, but the voter wishes to change one or more selections, the paper record must be voided so a new paper record can be created to compare to the new summary screen displayed after the voter changes his or her ballot selections.
 - In the event the selections do not match between the summary screen and the paper record, the voter shall immediately request assistance from a poll worker. A non-match could indicate a potential voting machine or printer malfunction.
- b. The voting equipment shall, in the presence of the voter, mark the paper record as being approved by the voter if the ballot selections are accepted; or voided or if the voter decides to change one or more selections.
- c. If the records do not match, the voting equipment shall mark and preserve the paper record and shall provide a means to preserve the corresponding electronic record so the source of error or malfunction can be analyzed.
- Discussion: The voting machine shall be withdrawn from service immediately and its use discontinued in accordance with jurisdiction procedures.
- d. The voting machine shall not record the electronic record until the paper record has been approved by the voter.
- e. Vendor documentation shall include procedures to enable the election official to return a voting machine to correct operation after a voter has used it incompletely or incorrectly. **This procedure shall not cause discrepancies between the tallies of the electronic and paper records.**

7.9.3 Electronic and Paper Record Structure

- a. All cryptographic software in the voting system shall be approved by the U.S. Government's Cryptographic Module Validation Program, as applicable.

Discussion: Cryptographic software may be used for a number of different purposes, including calculating checksums, encrypting records, authentication, generating random numbers, and digital signatures. This software should be reviewed and approved by the Cryptographic Module Validation Program (CMVP). There may be cryptographic voting schemes where the cryptographic algorithms used are necessarily different from any algorithms that have approved CMVP implementations, thus CMVP approved software should be used where feasible but is not required. The CMVP website is <http://csrc.nist.gov/cryptval>.

b. The electronic ballot image and paper records shall include information about the election.

- i. The voting equipment shall be able to include an identification of the particular election, the voting site and precinct, and the voting machine.

Discussion: If the voting site and precinct are different, both should be included.

- ii. The records shall include information identifying whether the balloting is provisional, early, or on election day, and information that identifies the ballot style in use.
- iii. The records shall include a voting session identifier that is generated when the voting equipment is placed in voting mode, and that can be used to identify the records as being created during that voting session.

Discussion: If there are several voting sessions on the same voting machine on the same day, the voting session identifiers must be different. They should be generated from a random number generator.

c. The electronic ballot image and paper records shall be linked by including a unique identifier within each record that can be used to identify each record uniquely and each record's corresponding record.

Discussion: The identifier serves the purpose of uniquely identifying and linking the records for cross-checking.

d. The voting machine should generate and store a digital signature for each electronic record.

e. The electronic ballot image records shall be able to be exported for auditing or analysis on standards-based and /or COTS information technology computing platforms.

- i. The exported electronic ballot image records shall be in a publicly available, non-proprietary format.

Discussion: It is advantageous when all electronic records, regardless of manufacturer, use the same format or can easily be converted to a publicly available, non-proprietary format; for example, the OASIS Election Markup Language (EML) Standard.

- ii. The records should be exported with a digital signature, which shall be calculated on the entire set of electronic records and their associated digital signatures.

Discussion: This is necessary to determine if records are missing or substituted.

- iii. The voting system vendor shall provide documentation as to the structure of the exported ballot image records and how they shall be read and processed by software.
 - iv. The voting system vendor shall provide a software program that will display the exported ballot image records and that may include other capabilities such as providing vote tallies and indications of undervotes.
 - v. The voting system vendor shall provide full documentation of procedures for exporting electronic ballot image records and reconciling those records with the paper audit records.
- f. The paper record should be created in a format that may be made available across different manufacturers of electronic voting systems.

Discussion: There may be a future requirement for some commonality in the format of paper records.

- g. The paper record shall be created such that its contents are machine readable.

Discussion: This can be done by using specific OCR fonts or barcodes.

- i. The paper record shall contain error correcting codes for the purpose of detecting read errors and for preventing other markings on the paper record from being misinterpreted when machine reading the paper record.

Discussion: This requirement is not mandatory if a state prohibits the paper record from containing any information that cannot be read and understood by the voter. This requirement serves the purpose of detecting scanning errors and preventing stray or deliberate markings on the paper from being interpreted as valid data.

- h. If barcode is used, the voting equipment shall be able to print a barcode with each paper record that contains the human-readable contents of the paper record.

Discussion: This requirement is not mandatory if a state prohibits the paper record from containing any information that cannot be read and understood by the voter.

- i. The barcode shall use an industry standard format and shall be able to be read using readily available commercial technology.

Discussion: Examples of such codes are Maxi Code or PDF417.

- ii. If the corresponding electronic record contains a digital signature, the digital signature shall be included in the barcode on the paper record.

- iii. The barcode shall not contain any information other than the paper record's human-readable content, error correcting codes, and digital signature information.

7.9.4 Equipment Security and Reliability

- a. The voting machine shall provide a standard, publicly documented printer port (or the equivalent) using a standard communication protocol.

Discussion: Using a standard, publicly documented printer protocol assists in security evaluations of system software.

- b. Tamper-evident seals or physical security measures shall protect the connection between the printer and the voting machine.
- c. If the connection between the voting machine and the printer has been broken, the voting machine shall detect this event and record it in the DRE internal audit log.
- d. The paper path between the printing, viewing and storage of the paper record shall be protected and sealed from access except by authorized election officials.
- e. The printer shall not be permitted to communicate with any system or machine other than the voting machine to which it is connected.
- f. The printer shall only be able to function as a printer; it shall not contain any other services (e.g., provide copier or fax functions) or network capability.
- g. The voting machine shall detect errors and malfunctions such as paper jams or low supplies of consumables such as paper and ink that may prevent paper records from being correctly displayed, printed or stored.

Discussion: This could be accomplished in a variety of different ways; for example, a printer that is out of paper or jammed could issue a different audible alarm for each condition.

- h. If an error or malfunction occurs, the voting machine shall suspend voting operations and should present a clear indication to the voter and election officials of the malfunction.
- i. The voting machine shall not record votes if an error or malfunction occurs.
- j. Printing devices should contain sufficient supplies of paper and ink to avoid reloading or opening equipment covers or enclosures and thus potential circumvention of security features; or be able to reload paper and ink with minimal disruption to voting and without circumvention of security features such as seals.

- k. Vendor documentation shall include procedures for investigating and resolving printer malfunctions including, but not limited to; printer operations, misreporting of votes, unreadable paper records, and power failures.
- l. Vendor documentation shall include printer reliability specifications including Mean Time Between Failure estimates, and shall include recommendations for appropriate quantities of backup printers and supplies.
- m. Protective coverings intended to be transparent on voting equipment shall be maintainable via a predefined cleaning process. If the coverings become damaged such that they obscure the paper record, they shall be replaceable.
- n. The paper record shall be sturdy, clean, and of sufficient durability to be used for verifications, reconciliations, and recounts conducted manually or by automated processing.

7.9.5 Preserving Voter Privacy

VVPAT records can be printed and stored by two different methods:

- Printed and stored on a continuous spool-to-spool paper roll where the voter views the paper record in a window
- Printed on separate pieces of paper, which are deposited in a secure receptacle.

If a requirement applies to only one method, that will be specified. Otherwise, the requirement applies to both.

- a. Voter privacy shall be preserved during the process of recording, verifying and auditing his or her ballot selections.

Discussion: The privacy requirements from Section 3 also apply to voting equipment with VVPAT.

- b. When a VVPAT with a spool-to-spool continuous paper record is used, a means shall be provided to preserve the secrecy of the paper record of voter selections.
- c. When a VVPAT with a spool-to-spool continuous paper record is used, no record shall be maintained of which voters used which voting machine or the order in which they voted.
- d. The electronic and paper records shall be created and stored in ways that preserve the privacy of the voter.

Discussion: For VVPAT systems that use separate pieces of paper for the record, this can be accomplished in various ways including shuffling the order of the records or other methods to separate the order of stored records.

- e. The privacy of voters whose paper records contain an alternative language shall be maintained.
- f. Unique identifiers shall not be displayed in a way that is easily memorable by the voter.

Discussion: Unique identifiers on the paper record are displayed or formatted in such a way that they are not memorable to voters, such as by obscuring them in other characters.

- g. Both paper rolls and paper record secure receptacles shall be controlled, protected, and preserved with the same security as a ballot box.

7.9.6 VVPAT Usability

- a. All usability requirements from Subsection 3.1 shall apply to voting machines with VVPAT.

Discussion: The requirements in this section are in addition to those in Subsection 3.1.

- b. The voting equipment shall be capable of showing the information on the paper in a font size of at least 3.0 mm and should be capable of showing the information in at least two font ranges; 3.0-4.0 mm, and 6.3-9.0 mm, under control of the voter or poll worker.

Discussion: In keeping with requirements in Subsection 3.1, the paper record should use the same font sizes as displayed by the voting machine, but at least be capable of 3.0 mm. While larger font sizes may assist voters with poor vision, certain disabilities such as tunnel vision are best addressed by smaller font sizes.

- c. The voting equipment shall display, print and store the paper record in any of the written alternative languages chosen for the ballot.
 - i. To assist with manual auditing, candidate names on the paper record shall be presented in the same language as used on the DRE summary screen.
 - ii. Information on the paper record not needed by the voter to perform verification shall be in English.

Discussion: In addition to the voter ballot selections, the marking of the paper record as accepted or void, and the indication of the ballot page number need to be printed in the alternative language. Other information, such as precinct and election identifiers, shall be in English to facilitate use of the paper record for auditing.

- d. The paper and electronic records shall be presented to allow the voter to read and compare the records without the voter having to shift his or her position.
- e. If the paper record cannot be displayed in its entirety on a single page, a means shall be provided to allow the voter to view the entire record.

Discussion: Possible solutions include scrolling the paper or printing a new sheet of paper. The voter should be notified if it is not possible to scroll in reverse, so they will know to complete verification in one pass.

- f. If the paper record cannot be displayed in its entirety on a single page, each page of the record shall be numbered and shall include the total count of pages for the record.

Discussion: Possible numbering schemes include “Page X of Y.”

- g. The instructions for performing the verification process shall be made available to the voter in a location on the voting machine.

Discussion: All instructions must meet the usability requirements contained in Subsection 3.1.

7.9.7 VVPAT Accessibility

- a. All accessibility requirements from Subsection 3.2 shall apply to voting machines with VVPAT.
- b. If the normal voting procedure includes VVPAT, the accessible voting equipment should provide features that enable voters who are visually impaired and voters with an unwritten language to perform this verification. If state statute designates the paper record produced by the VVPAT to be the official ballot or the determinative record on a recount, the accessible voting equipment shall provide features that enable visually impaired voters and voters with an unwritten language to review the paper record.

Discussion: For example, the accessible voting equipment might provide an automated reader that converts the paper record contents into audio output.

8 Quality Assurance Requirements

Table of Contents

8	Quality Assurance Requirements.....	147
8.1	Scope	147
8.2	General Requirements	147
8.3	Components from Third Parties	148
8.4	Responsibility for Tests	148
8.5	Parts and Materials Special Tests and Examinations	148
8.6	Quality Conformance Inspections	148
8.7	Documentation	149

[Intentionally left blank]

8 Quality Assurance Requirements

8.1 Scope

Quality assurance provides continuous confirmation that a voting system conforms with the *Guidelines* and to the requirements of state and local jurisdictions. Quality assurance is a vendor function that is initiated prior to system development and continues throughout the maintenance life cycle of the voting system. Quality assurance focuses on building quality into a voting system and reducing dependence on system tests at the end of the life cycle to detect deficiencies, thus helping ensure the system:

- Meets stated requirements and objectives
- Adheres to established standards and conventions
- Functions consistently with related components and meets dependencies for use within the jurisdiction
- Reflects all changes approved during its initial development, internal testing, national certification, and, if applicable, state certification processes

8.2 General Requirements

The voting system vendor is responsible for designing and implementing a quality assurance program to ensure that the design, workmanship, and performance requirements are achieved in all delivered systems and components. At a minimum, this program shall:

- a. Include procedures for specifying, procuring, inspecting, accepting, and controlling parts and raw materials of the requisite quality
- b. Require the documentation of the hardware and software development process
- c. Identify and enforce all requirements for:
 - i. In-process inspection and testing that the manufacturer deems necessary to ensure proper fabrication and assembly of hardware
 - ii. Installation and operation of software and firmware
- d. Include plans and procedures for post-production environmental screening and acceptance testing
- e. Include a procedure for maintaining all data and records required to document and verify the quality inspections and tests

8.3 Components from Third Parties

A vendor who does not manufacture all the components of its voting system, but instead procures components as standard commercial items for assembly and integration into a voting system, shall verify that the supplier vendors follow documented quality assurance procedures that are at least as stringent as those used internally by the voting system vendor.

8.4 Responsibility for Tests

The manufacturer or vendor shall be responsible for performing all quality assurance tests, acquiring and documenting test data, and providing test reports for examination by the test lab as part of the national certification process. These reports shall also be provided to the purchaser upon request.

8.5 Parts and Materials Special Tests and Examinations

In order to ensure that voting system parts and materials function properly, vendors shall:

- a. Select parts and materials to be used in voting systems and components according to their suitability for the intended application. Suitability may be determined by similarity of this application to existing standard practice or by means of special tests
- b. Design special tests, if needed, to evaluate the part or material under conditions accurately simulating the actual voting system operating environment
- c. Maintain the resulting test data as part of the quality assurance program documentation

8.6 Quality Conformance Inspections

The vendor performs conformance inspections to ensure the overall quality of the voting system and components delivered to the test lab for national certification testing and to the jurisdiction for implementation.

To meet the conformance inspection requirements the vendor or manufacturer shall:

- a. Inspect and test each voting system or component to verify that it meets all inspection and test requirements for the system
- b. Deliver a record of tests or a certificate of satisfactory completion with each system or component

8.7 Documentation

Vendors are required to produce documentation to support the independent testing required for their products to be granted national certification. Volume II, Section 2, Description of the Technical Data Package, identifies the documentation required for the national certification testing process. This documentation shall be sufficient to serve the needs of the test lab, election officials, and maintenance technicians. It shall be prepared and published in accordance with standard commercial practice for information technology and electronic and mechanical equipment. It shall include, at a minimum, the following:

- System overview
- System functionality description
- System hardware specification
- Software design and specifications
- System security specification
- System test and verification specification
- System operations procedures
- System maintenance procedures
- Personnel deployment and training requirements
- Configuration management plan
- Quality assurance program
- System change notes

[Intentionally left blank]

9 Configuration Management Requirements

Table of Contents

9	Configuration Management Requirements	153
9.1	Scope	153
9.1.1	Configuration Management Requirements	153
9.1.2	Organization of Configuration Management Requirements	153
9.1.3	Application of Configuration Management Requirements	154
9.2	Configuration Management Policy	154
9.3	Configuration Identification	154
9.3.1	Classification and Naming Configuration Items	154
9.3.2	Versioning Conventions	155
9.4	Baseline and Promotion Procedures	155
9.5	Configuration Control Procedures	155
9.6	Release Process	156
9.7	Configuration Audits	156
9.7.1	Physical Configuration Audit	156
9.7.2	Functional Configuration Audit	157
9.8	Configuration Management Resources	157

[Intentionally left blank]

9 Configuration Management Requirements

9.1 Scope

This section contains specific requirements for configuration management of voting systems. For the purpose of the *Guidelines*, configuration management is defined as a set of activities and associated practices that ensures full knowledge and control of the components of a system, starting with its initial development and progressing through its ongoing maintenance and enhancement. This section describes activities in terms of their purposes and outcomes. It does not describe specific procedures or steps to be employed to accomplish them. Specific steps and procedures are left to the vendor to select.

Vendors are required to submit these procedures as part of the Technical Data Package for system certification. State or local election legislation, regulations, or contractual agreements may require the vendor to conform to additional requirements for configuration management or to adopt specific required procedures. EAC and state and local election officials reserve the right to inspect vendor facilities and operations to determine conformance with the vendor's reported procedures and with these requirements.

9.1.1 Configuration Management Requirements

Configuration management addresses a broad set of record keeping, auditing, and reporting activities that contribute to full knowledge and control of a system and its components. These activities include:

- Identifying discrete system components
- Creating records of a formal baseline and later versions of components
- Controlling changes made to the system and its components
- Releasing new versions of the system
- Auditing the system, including its documentation, against configuration management records
- Controlling interfaces to other systems
- Identifying tools used to build and maintain the system

9.1.2 Organization of Configuration Management Requirements

The requirements for configuration management include:

- Application of configuration management requirements
- Configuration management policy
- Configuration identification

- Baseline, promotion, and demotion procedures
- Configuration control procedures
- Release process
- Configuration audits
- Configuration management resources

9.1.3 Application of Configuration Management Requirements

Requirements for configuration management apply to all components of voting systems regardless of the specific technologies employed. These components include:

- Software
- Hardware
- Communications
- Documentation
- Identification and naming conventions (including changes to these conventions) for software programs and data files
- Development and testing artifacts such as test data and scripts
- File archiving and data repositories

9.2 Configuration Management Policy

The vendor shall describe its policies for configuration management in the Technical Data Package. This description shall address the following elements:

- Scope and nature of configuration management program activities
- Breadth of application of the vendor's policies and practices to the voting system, i.e., extent to which policies and practices apply to the total system, and extent to which policies and practices of suppliers apply to particular components, subsystems or other defined system elements

9.3 Configuration Identification

Configuration identification is the process of identifying, naming, and acquiring configuration items. Configuration identification encompasses all system components.

9.3.1 Classification and Naming Configuration Items

The vendor shall describe the procedures and conventions used to classify configuration items into categories and subcategories, uniquely number or otherwise identify configuration items and name configuration items.

9.3.2 Versioning Conventions

When a system component is part of a higher level system element such as a subsystem, the vendor shall describe the conventions used to:

- a. Identify the specific versions of individual configuration items and sets of items that are incorporated in higher level system elements such as subsystems
- b. Uniquely number or otherwise identify versions
- c. Name versions

9.4 Baseline and Promotion Procedures

The vendor shall establish formal procedures and conventions for establishing and providing a complete description of the procedures and related conventions used to:

- a. Establish a particular instance of a component as the starting baseline
- b. Promote subsequent instances of a component to baseline status as development progresses through to completion of the initial completed version released to the accredited test lab for testing
- c. Promote subsequent instances of a component to baseline status as the component is maintained throughout its life cycle until system retirement (i.e., the system is no longer sold or maintained by the vendor)

9.5 Configuration Control Procedures

Configuration control is the process of approving and implementing changes to a configuration item to prevent unauthorized additions, changes or deletions. The vendor shall establish such procedures and related conventions, providing a complete description of those procedures used to:

- a. Develop and maintain internally developed items
- b. Acquire and maintain third-party items
- c. Resolve internally identified defects for items regardless of their origin
- d. Resolve externally identified and reported defects (i.e., by customers and accredited test labs)

9.6 Release Process

The release process is the means by which the vendor installs, transfers or migrates the system to the accredited test lab and, eventually, to its customers. The vendor shall establish such procedures and related conventions, providing a complete description of those used to:

- a. Perform a first release of the system to an accredited test lab
- b. Perform a subsequent maintenance or upgrade release of the system or particular components, to an accredited test lab
- c. Perform the initial delivery and installation of the system to a customer, including confirmation that the installed version of the system matches exactly the certified system version
- d. Perform a subsequent maintenance or upgrade release of the system or a particular component to a customer, including confirmation that the installed version of the system matches exactly the certified system version

9.7 Configuration Audits

The *Guidelines* require two types of configuration audits: Physical Configuration Audits (PCA) and Functional Configuration Audits (FCA).

9.7.1 Physical Configuration Audit

The Physical Configuration Audit is conducted by the accredited test lab to compare the voting system components submitted for certification to the vendor's technical documentation.

For the PCA, a vendor shall provide:

- a. Identification of all items that are to be a part of the software release
- b. Specification of compiler (or choice of compilers) to be used to generate executable programs
- c. Identification of all hardware that interfaces with the software
- d. Configuration baseline data for all hardware that is unique to the system
- e. Copies of all software documentation intended for distribution to users, including program listings, specifications, operations manual, voter manual, and maintenance manual

- f. User acceptance test procedures and acceptance criteria
- g. Identification of any changes between the physical configuration of the system submitted for the PCA and that submitted for the FCA, with a certification that any differences do not degrade the functional characteristics
- h. Complete descriptions of its procedures and related conventions used to support this audit by:
 - i. Establishing a configuration baseline of the software and hardware to be tested
 - ii. Confirming whether the system documentation matches the corresponding system components

9.7.2 Functional Configuration Audit

The Functional Configuration Audit is conducted by the accredited test lab to verify that the system performs all the functions described in the system documentation. The vendor shall:

- a. Completely describe its procedures and related conventions used to support this audit for all system components
- b. Provide the following information to support this audit:
 - i. Copies of all procedures used for module or unit testing, integration testing, and system testing
 - ii. Copies of all test cases generated for each module and integration test, and sample ballot formats or other test cases used for system tests
 - iii. Records of all tests performed by the procedures listed above, including error corrections and retests

In addition to such audits performed by the accredited test lab during the national certification process, elements of this audit may also be performed by state election organizations during the system certification process and individual jurisdictions during system acceptance testing.

9.8 Configuration Management Resources

Often, configuration management activities are performed with the aid of automated tools. Assuring that such tools are available throughout the system life cycle—including whether the vendor is acquired by or merged with another organization—is critical to effective configuration management. Vendors may choose the specific tools they use to perform the record keeping, auditing, and reporting activities of the configuration management standards.

The resources documentation requirements focus on assuring that procedures are in place to record information about the tools to help ensure that they, and the data they contain, can be transferred effectively and promptly to a third party should the need arise. Within this context, a vendor is required to develop and provide a complete description of the procedures and related practices for maintaining information about:

- a. Specific tools used, current version, and operating environment specifications
- b. Physical location of the tools, including designation of computer directories and files
- c. Procedures and training materials for using the tools

Appendix A: Glossary

Table of Contents

A	Glossary	A-3
A.1	Glossary	A-3
A.2	Sources	A-20

[Intentionally left blank]

Appendix A: Glossary

This glossary contains terms needed to understand voting systems and related areas such as security, human factors, and testing. Sources consulted in preparing the definitions are listed in section A.2.

A.1 Glossary

A

abandoned ballot: Ballot that the voter did not place in the ballot box or record as cast on DRE before leaving the polling place

absentee ballot: Ballot cast by a voter unable to vote in person at his or her polling place on election day

acceptance testing: Examination of a voting system and its components by the purchasing election authority (usually in a simulated-use environment) to validate performance of delivered units in accordance with procurement requirements, and to validate that the delivered system is, in fact, the certified system purchased

Access Board: Independent federal agency whose primary mission is accessibility for people with disabilities and a leading source of information on accessible design

accessibility: Measurable characteristics that indicate the degree to which a system is available to, and usable by, individuals with disabilities. The most common disabilities include those associated with vision, hearing and mobility, as well as cognitive disabilities.

accessible voting station: Voting station equipped for individuals with disabilities

accreditation: Formal recognition that a laboratory is competent to carry out specific tests or calibrations

accreditation body: (1) Authoritative body that performs accreditation (2) An independent organization responsible for assessing the performance of other organizations against a recognized standard, and for formally confirming the status of those that meet the standard

accuracy: (1) Extent to which a given measurement agrees with an accepted standard for that measurement (2) Closeness of the agreement between the result of a measurement and a true value of the particular quantity subject to measurement. Accuracy is a qualitative concept and is not interchangeable with precision.

accuracy for voting systems: Ability of the system to capture, record, store, consolidate and report the specific selections and absence of selections, made by the voter for each ballot position without error. Required accuracy is defined in terms of an error rate that for testing purposes represents the maximum number of errors allowed while processing a specified volume of data.

adequate security: Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, unauthorized access to, or modification of, information. This includes ensuring that systems and applications operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.

alternative format: The ballot or accompanying information is said to be in an alternative format if it is in a representation other than the standard ballot language and format. Examples include, but are not limited to languages other than English, Braille, ASCII text, large print, recorded audio.

audio ballot: a ballot in which a set of offices is presented to the voter in spoken, rather than written, form

audio-tactile interface (ATI): Voter interface designed to not require visual reading of a ballot. Audio is used to convey information to the voter and sensitive tactile controls allow the voter to communicate ballot selections to the voting system.

audit: Systematic, independent, documented process for obtaining records, statements of fact or other relevant information and assessing them objectively to determine the extent to which specified requirements are fulfilled

audit trail: Recorded information that allows election officials to review the activities that occurred on the voting equipment to verify or reconstruct the steps followed without compromising the ballot or voter secrecy

audit trail for direct-recording equipment: Paper printout of votes cast, produced by direct-recording electronic (DRE) voting machines, which election officials may use to crosscheck electronically tabulated totals

availability: The percentage of time during which a system is operating properly and available for use

B

ballot: The official presentation of all of the contests to be decided in a particular election. See also, **audio ballot**, **ballot image**, **video ballot**, **electronic voter interface**.

ballot configuration: Particular set of contests to appear on the ballot for a particular election district, their order, the list of ballot positions for each contest, and the binding of candidate names to ballot positions

ballot counter: Process in a voting device that counts the votes cast in an election

ballot counting logic: The software logic that defines the combinations of voter choices that are valid and invalid on a given ballot and that determines how the vote choices are totaled in a given election

ballot format: The concrete presentation of the contents of a ballot appropriate to the particular voting technology being used. The contents may be rendered using various methods of presentation (visual or audio), language or graphics.

ballot image: Electronically produced record of all votes cast by a single voter. See also **cast vote record**.

ballot instructions: Information provided to the voter during the voting session that describes the procedure for executing a ballot. Such material may (but need not) appear directly on the ballot.

ballot measure: (1) A question that appears on the ballot for approval or rejection. (2) A contest on a ballot where the voter may vote yes or no.

ballot position: A specific place in a ballot where a voter's selection for a particular contest may be indicated. Positions may be connected to row and column numbers on the face of a voting machine or ballot, particular bit positions in a binary record of a ballot (for example, an electronic ballot image), the equivalent in some other form. Ballot positions are bound to specific contests and candidate names by the ballot configuration.

ballot preparation: Selecting the specific contests and questions to be contained in a ballot format and related instructions; preparing and testing election-specific software containing these selections; producing all possible ballot formats; and validating the correctness of ballot materials and software containing these selections for an upcoming election

ballot production: Process of generating ballots for presentation to voters, e.g., printing paper ballots or configuring the ballot presentation on a DRE

ballot rotation: Process of varying the order of the candidate names within a given contest

ballot scanner: Device used to read the voter selection data from a paper ballot or ballot card

ballot style: See **ballot configuration**

C

candidate: Person contending in a contest for office. A candidate may be explicitly presented as one of the choices on the ballot or may be a write-in candidate.

candidate register: Record that reflects the total votes cast for the candidate. This record is augmented as each ballot is cast on a DRE or as digital signals from the conversion of voted paper ballots are logically interpreted and recorded.

canvass: Compilation of election returns and validation of the outcome that forms the basis of the official results by political subdivision

cast ballot: Ballot that has been deposited by the voter in the ballot box or electronically submitted for tabulation

cast vote record: Permanent record of all votes produced by a single voter whether in electronic, paper or other form. Also referred to as ballot image when used to refer to electronic ballots.

catastrophic system failure: Total loss of function or functions, such as the loss or unrecoverable corruption of voting data or the failure of an on board battery of volatile memory

central count voting system: A voting system that tabulates ballots from multiple precincts at a central location. Voted ballots are placed into secure storage at the polling place. Stored ballots are transported or transmitted to a central counting place which produces the vote count report.

certification: Procedure by which a third party gives written assurance that a product, process or service conforms to specified requirements. See also **state certification** and **national certification**.

certification testing: Testing performed under either national or state certification processes to verify voting system conformance to requirements

challenged ballot: Ballot provided to an individual who claim they are registered and eligible to vote but whose eligibility or registration status cannot be confirmed when they present themselves to vote. Once voted, such ballots must be kept separate from other ballots and are not included in the tabulation until after the voter's eligibility is confirmed. Michigan is an exception in that they determine voter eligibility before a ballot is issued. See also **provisional ballot**

checksum: Value computed from the content of a document or data record. Typically this is the sum of the numeric representations of all the characters in the text. Checksums are used to aid in detecting errors or alterations during transmission or storage.

claim of conformance: Statement by a vendor declaring that a specific product conforms to a particular standard or set of standard profiles; for voting systems, NASED qualification or EAC certification provides independent verification of a claim

closed primary: Primary election in which voters receive a ballot listing only those candidates running for office in the political party with which the voters are affiliated. In some states, non-partisan contests and ballot issues may be included. In some cases, political parties may allow unaffiliated voters to vote in their party's primary

commercial off-the-shelf (COTS): Commercial, readily available hardware devices (such as card readers, printers or personal computers) or software products (such as operating systems, programming language compilers, or database management systems)

Common Industry Format (CIF): Refers to the format described in ANSI/INCITS 354-2001 "Common Industry Format (CIF) for Usability Test Reports

component: Element within a larger system; a component can be hardware or software. For hardware, it is a physical part of a subsystem that can be used to compose larger systems (e.g., circuit boards, internal modems, processors, computer memory). For software, it is a module of executable code that performs a well-defined function and interacts with other components.

confidentiality: Prevention of unauthorized disclosure of information

configuration management: Discipline applying technical and administrative direction and surveillance to identify and document functional and physical characteristics of a configuration item, control changes to these characteristics, record and report change processing and implementation status, and verify compliance with specified requirements

configuration management plan: Document detailing the process for identifying, controlling and managing various released items (such as code, hardware and documentation)

configuration status accounting: An element of configuration management, consisting of the recording and reporting of information needed to manage a configuration effectively. This includes a listing of the approved configuration identification, the status of proposed changes to the configuration, and the implementation status of approved changes.

conformance: Fulfillment of specified requirements by a product, process or service

conformance testing: Process of testing an implementation against the requirements specified in one or more standards. The outcomes of a conformance test are generally a pass or fail result, possibly including reports of problems encountered during the execution. Also known as certification testing.

contest: Decision to be made within an election, which may be a contest for office or a referendum, proposition and/or question. A single ballot may contain one or more contests.

count: Process of totaling votes. See **tabulation**.

counted ballot: Ballot that has been processed and whose votes are included in the candidates and measures vote totals

corrective action: Action taken to eliminate the causes of an existing deficiency or other undesirable situation in order to prevent recurrence

cross filing: Endorsement of a single candidate or slate of candidates by more than one political party. The candidate or slate appears on the ballot representing each endorsing political party. Also referred to as cross-party endorsement.

cryptographic key: Value used to control cryptographic operations, such as decryption, encryption, signature generation or signature verification

cryptography: Discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, prevent their undetected modification and establish their authenticity

cumulative voting: A method of voting exclusive to multi-member district election (e.g. county board) in which each voter may cast as many votes as there are seats to be filled and may cast two or more of those votes for a single candidate

D

data accuracy: (1) Data accuracy is defined in terms of ballot position error rate. This rate applies to the voting functions and supporting equipment that capture, record, store, consolidate and report the specific selections, and absence of selections, made by the voter for each ballot position. (2) The system's ability to process voting data absent internal errors generated by the system. It is distinguished from data integrity, which encompasses errors introduced by an outside source.

data integrity: Invulnerability of the system to accidental intervention or deliberate, fraudulent manipulation that would result in errors in the processing of data. It is distinguished from data accuracy that encompasses internal, system-generated errors.

decertification: Revocation of national or state certification of voting system hardware and software

decryption: Process of changing encrypted text into plain text

device: Functional unit that performs its assigned tasks as an integrated whole

digital signature: An asymmetric key operation where the private key is used to digitally sign an electronic document and the public key is used to verify the signature. Digital signatures provide data authentication and integrity protection

direct-recording electronic (DRE) voting system: An electronic voting system that utilizes electronic components for the functions of ballot presentation, vote capture, vote recording,

and tabulation which are logically and physically integrated into a single unit. A DRE produces a tabulation of the voting data stored in a removable memory component and in printed hardcopy.

directly verifiable: Voting system feature that allows the voter to verify at least one representation of his or her ballot with his/her own senses, not using any software or hardware intermediary. Examples include a marksense paper ballot and a DRE with a voter verifiable paper record feature.

disability: With respect to an individual; (1) a physical or mental impairment that substantially limits one or more of the major life activities of such individual; (2) a record of such an impairment; (3) being regarded as having such an impairment (definition from the Americans with Disabilities Act).

dynamic voting system software: Software that changes over time once it is installed on the voting equipment. See also voting system software.

E

EAC: Election Assistance Commission (www.eac.gov)

early voting: Broadly, voting conducted before election day where the voter completes the ballot in person at a county office or other designated polling place or ballot drop site prior to election day

election: A formal process of selecting a person for public office or of accepting or rejecting a political proposition by voting

election databases: Data file or set of files that contain geographic information about political subdivisions and boundaries, all contests and questions to be included in an election, and the candidates for each contest

election definition: Definition of the contests and questions that will appear on the ballot for a specific election

election district: Contiguous geographic area represented by a public official who is elected by voters residing within the district boundaries. The district may cover an entire state or political subdivision, may be a portion of the state or political subdivision, or may include portions of more than one political subdivision.

election management system: Set of processing functions and databases within a voting system that defines, develops and maintains election databases, performs election definitions and setup functions, format ballots, count votes, consolidates and report results, and maintains audit trails

election officials: The people associated with administering and conducting elections, including government personnel and poll workers

election programming: Process by which election officials or their designees use voting system software to logically define the ballot for a specific election

electronic cast vote record: An electronic version of the cast vote record

electronic voter interface: Subsystem within a voting system which communicates ballot information to a voter in video, audio or other alternative format which allows the voter to select candidates and issues by means of vocalization or physical actions

electronic voting machine: Any system that utilizes an electronic component. Term is generally used to refer to DREs. See also **voting equipment**, **voting system**.

electronic voting system: An electronic voting system is one or more integrated devices that utilize an electronic component for one or more of the following functions: ballot presentation, vote capture, vote recording, and tabulation. A DRE is a functionally and physically integrated electronic voting system which provides all four functions electronically in a single device. An optical scan (also known as marksense) system where the voter marks a paper ballot with a marking instrument and then deposits the ballot in a tabulation device is partially electronic in that the paper ballot provides the presentation, vote capture and vote recording functions. An optical scan system employing a ballot marking device adds a second electronic component for ballot presentation and vote capture functions.

encryption: Process of obscuring information by changing plain text into ciphertext for the purpose of security or privacy. See also **cryptography** and **decryption**.

error correcting code: coding system that allows data being read or transmitted to be checked for errors and, when detected, corrects those errors

F

Federal Information Processing Standards: Standards for federal computer systems developed by NIST. These standards are developed when there are no existing industry standards to address federal requirements for system interoperability, portability of data and software, and computer security.

firmware: Computer programming stored in programmable read-only memory thus becoming a permanent part of the computing device. It is created and tested like software.

Functional Configuration Audit (FCA): Exhaustive verification of every system function and combination of functions cited in the vendor's documentation. The FCA verifies the accuracy and completeness of the system's Voter Manual, Operations Procedures, Maintenance Procedures, and Diagnostic Testing Procedures.

functional test: Test performed to verify or validate the accomplishment of a function or a series of functions

G

general election: Election in which voters, regardless of party affiliation, are permitted to select candidates to fill public office and vote on ballot issues

guidelines: See **product standard**

H

hash: Algorithm that maps a bit string of arbitrary length to a fixed-length bit string.

hash function: A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties: 1. (One-way) It is computationally infeasible to find any input that maps to any pre-specified output, and 2. (Collision resistant) It is computationally infeasible to find any two distinct inputs that map to the same output.

I

indirectly verifiable: Voting system feature that allows a voter to verify his or her selections via a hardware or software intermediary. An example is a touch screen DRE where the voter verifies the ballot selections through the assistance of audio stimuli.

implementation statement: Statement by a vendor indicating the capabilities, features, and optional functions as well as extensions that have been implemented. Also known as implementation conformance statement.

Independent Testing Authority (ITA): Replaced by “accredited testing laboratories” and “test labs.” Prior usage referred to independent testing organizations accredited by the National Association of State Election Directors (NASD) to perform voting system qualification testing.

information security: Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability

inspection: Examination of a product design, product, process or installation and determination of its conformity with specific requirements or, on the basis of professional judgment, with general requirements. Inspection of a process may include inspection of staffing, facilities, technology and methodology.

integrity: Guarding against improper information modification or destruction, and ensuring information non-repudiation and authenticity

internal audit log: A human readable record, resident on the voting machine, used to track all activities of that machine. This log records every activity performed on or by the machine indicating the event and when it happened.

K

key management: Activities involving the handling of cryptographic keys and other related security parameters (e.g., passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and zeroization.

L

logic and accuracy testing: Testing of the tabulator setups of a new election definition to ensure that the content correctly reflects the election being held (i.e., contests, candidates, number to be elected, ballot styles) and that all voting positions can be voted for the maximum number of eligible candidates and that results are accurately tabulated and reported.

logical correctness: Condition signifying that, for a given input, a computer program will satisfy the program specification and produce the required output

M

marksense: System by which votes are recorded by means of marks made in voting response fields designated on one or both faces of a ballot card or series of cards. Marksense systems may use an optical scanner or similar sensor to read the ballots. Also known as optical scan.

measure register: Record that reflects the total votes cast for and against a specific ballot issue. This record is augmented as each ballot is cast on a DRE or as digital signals from the conversion of voted paper ballots are logically interpreted and recorded.

mechanical lever voting machine: Machine that directly records a voter's choices via mechanical lever-actuated controls into a counting mechanism that tallies the votes without using a physical ballot

multi-seat contest: Contest in which multiple candidates can run, up to a specified number of seats. Voters may vote for no more than the specified number of candidates

N

NASED: National Association of State Election Directors, (www.nased.org)

national certification testing: Examination and testing of a voting system to determine if the system complies with the performance and other requirements of the national certification standards and with its own specifications

national certification test report: Report of results of independent testing of a voting system by an accredited test lab delivered to the EAC with a recommendation regarding granting a certification number

NIST: National Institute of Standards and Technology

non-partisan office: Elected office for which candidates run without political party affiliation

nonvolatile memory: Memory in which information can be stored indefinitely with no power applied. ROMs and PROMs are examples of nonvolatile memory.

NVLAP: The National Voluntary Laboratory Accreditation Program operated by NIST

O

open primary: Primary election in which any voters can participate, regardless of their political affiliation. Some states require voters to publicly declare their choice of party ballot at the polling place, after which the poll worker provides or activates the appropriate ballot. Other states allow the voters to make their choice of party ballot within the privacy of the voting booth.

operational environment: All software, hardware (including facilities, furnishings and fixtures), materials, documentation, and the interface used by the election personnel, maintenance operator, poll worker, and voter, required for voting equipment operations.

optical scan, optical scan system: System by which votes are recorded by means of marks made in voting response fields designated on one or both faces of a ballot card or series of cards. An optical scan system reads and tabulates ballots, usually paper ballots, by scanning the ballot and interpreting the contents. Also known as **marksense**.

overvote: Voting for more than the maximum number of selections allowed in a contest

P

paper-based voting system: Voting system that records votes, counts votes, and tabulates the vote count, using one or more ballot cards or paper ballots

paper record: Paper cast vote record that can be directly verified by a voter. See also **ballot image, cast vote record**.

partisan office: An elected office for which candidates run as representatives of a political party

personal assistive device: A device that is carried or worn by an individual with some physical impairment whose primary purpose is to help compensate for that impairment

Physical Configuration Audit (PCA): Inspection by an accredited test laboratory that compares the voting system components submitted for certification testing to the vendor's technical documentation and confirms that the documentation submitted meets the national certification requirements. Includes witnessing of the build of the executable system to ensure that the certified release is built from the tested components.

political subdivision: Any unit of government, such as counties and cities, school districts, and water and conservation districts having authority to hold elections for public offices or on ballot issues

polling location: Physical address of a polling place

polling place: Facility to which voters are assigned to cast in-person ballots

precinct: Election administration division corresponding to a contiguous geographic area that is the basis for determining which contests and issues the voters legally residing in that area are eligible to vote on

precinct count: Counting of ballots in the same precinct in which those ballots have been cast

precinct count voting system: a voting system that tabulates ballots at the polling place. These systems typically tabulate ballots as they are cast and print the results after the close of polling. For DREs, and for some paper-based systems, these systems provide electronic storage of the vote count and may transmit results to a central location over public telecommunication networks.

precision: (1) Extent to which a given set of measurements of the same sample agree with their mean. Thus, precision is commonly taken to be the standard deviation estimated from sets of duplicate measurements made under conditions of repeatability, that is, independent test results obtained with the same method on identical test material, in the same laboratory or test facility, by the same operator using the same equipment within short intervals of time. (2) Degree of refinement in measurement or specification, especially as represented by the number of digits given.

primary election: Election held to determine which candidate will represent a political party for a given office in the general election. Some states have an open primary, while others have a closed primary. Sometimes elections for nonpartisan offices and ballot issues are held during primary elections.

primary presidential delegation nomination: Primary election in which voters choose the delegates to the presidential nominating conventions allotted to their states by the national party committees

privacy: The ability to prevent others from determining how an individual voted

private key: The secret part of an asymmetric key pair that is typically used to digitally sign or decrypt data

product standard: Standard that specifies requirements to be fulfilled by a product or a group of products, to establish its fitness for purpose

provisional ballot: Ballot provided to individuals who claim they are registered and eligible to vote but whose eligibility or registration status cannot be confirmed when they present themselves to vote. Once voted, such ballots must be kept separate from other ballots and are not included in the tabulation until after the voter's eligibility is confirmed. In some jurisdictions called an affidavit ballot. See also **challenged ballot**.

public key: Public part of an asymmetric key pair that is typically used to verify digital signatures or encrypt data

public network direct-recording electronic (DRE) voting system: A DRE that transmits vote counts to a central location over a public telecommunication network

Q

qualification number: A number issued by NASED (National Association of State Election Directors) to a system that has been tested by an accredited Independent Testing Authority for compliance with the voting system standards. Issuance of a qualification number indicates that the system conforms to the national standards.

qualification test report: Report of results of independent testing of a voting system by an Independent Test Authority documenting the specific system configuration tested, the scope of tests conducted and when testing was completed.

qualification testing: Examination and testing of a voting system by a NASED-accredited Independent Test Authority to determine if the system conforms to the performance and other requirements of the national certification standards and the vendor's own specifications.

R

ranked order voting: Practice that allows voters to rank candidates in a contest in order of choice: 1, 2, 3 and so on. A candidate receiving a majority of the first choice votes wins that election. If no candidate receives a majority, the last place candidate is deleted, and all

ballots are counted again, with each ballot cast for the deleted candidate applied to the next choice candidate listed on the ballot. The process of eliminating the last place candidate and recounting the ballots continues until one candidate receives a majority of the vote. The practice is also known as instant runoff voting, preferences or preferential voting, or choice voting.

recall issue with options: Process that allows voters to remove elected representatives from office prior to the expiration of their terms of office. The recall may involve not only the question of whether a particular officer should be removed, but also the question of naming a successor in the event that there is an affirmative vote for the recall.

recertification: Re-examination, and possibly retesting of a voting system that was modified subsequent to receiving national and/or state certification. The object of is to determine if the system as modified still conforms to the requirements.

recount: Retabulation of the votes cast in an election

referendum: Process whereby a state law or constitutional amendment may be referred to the voters before it goes into effect

reproducibility: Ability to obtain the same test results by using the same test method on identical test items in different testing laboratories with different operators using different equipment

requirement: Provision that conveys criteria to be fulfilled

residual vote: Total number of votes that cannot be counted for a specific contest. There may be multiple reasons for residual votes (e.g., declining to vote for the contest, overvoting in a contest).

risk assessment: The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and safeguards that would mitigate this impact

runoff election: Election to select a winner following a primary or a general election, in which no candidate in the contest received the required minimum percentage of the votes cast. The two candidates receiving the most votes for the contest in question proceed to the runoff election.

S

secure receptacle: The container for storing VVPAT paper audit records

security analysis: An inquiry into the potential existence of security flaws in a voting system. Includes an analysis of the system's software, firmware, and hardware, as well as the procedures associated with system development, deployment, operation and management.

security controls: Management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

semi-static voting system software: Software that may change in response to the voting equipment on which it is installed or to election-specific programming.

split precinct: A precinct that contains an election district subdivision, e.g., a water district or school board district, requiring an additional ballot configuration

spoiled ballot: Ballot that has been voted but will not be cast

state certification: State examination and possibly testing of a voting system to determine its compliance with state requirements for voting systems

static voting system software: Software that does not change based on the election being conducted or the voting equipment upon which it is installed, e.g., executable code

straight party voting: Mechanism that allows voters to cast a single vote to select all candidates on the ballot from a single political party

support software: Software that aids in the development, maintenance, or use of other software, for example, compilers, loaders and other utilities

symmetric (secret) encryption algorithm: Encryption algorithms using the same secret key for encryption and decryption

T

tabulation: Process of totaling votes. See also **count**.

t-coil: Inductive coil used in some hearing aids to allow reception of an audio band magnetic field signal, instead of an acoustic signal. The magnetic or inductive mode of reception is commonly used in conjunction with telephones, auditorium loop systems and other systems that provide the required magnetic field output.

tabulator: Device that counts votes

technical data package: Vendor documentation relating to the voting system required to be submitted with the system as a precondition of certification testing

telecommunications: Transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received

test: Technical operation that consists of the determination of one or more characteristics of a given product, process or service according to a specified procedure

test campaign: Sum of the work by a voting system test lab on a single product or system from contract through test plan, conduct of testing for each requirement (including hardware, software, and systems), reporting, archiving, and responding to issues afterwards

testing standard: Standard that is concerned with test methods, sometimes supplemented with other provisions related to testing, such as sampling, use of statistical methods or sequence of tests

test method: Specified technical procedure for performing a test

test plan: Document created prior to testing that outlines the scope and nature of testing, items to be tested, test approach, resources needed to perform testing, test tasks, risks and schedule

touch screen voting machine: A voting machine that utilizes a computer screen to display the ballot and allows the voter to indicate his or her selections by touching designated locations on the screen

U

undervote: Occurs when the number of choices selected by a voter in a contest is less than the maximum number allowed for that contest or when no selection is made for a single choice contest

usability: Effectiveness, efficiency and satisfaction with which a specified set of users can achieve a specified set of tasks in a particular environment. Usability in the context of voting refers to voters being able to cast valid votes as they intended quickly, without errors, and with confidence that their ballot choices were recorded correctly. It also refers to the usability of the setup and operation in the polling place of voting equipment.

usability testing: Encompasses a range of methods that examine how users in the target audience actually interact with a system, in contrast to analytic techniques such as usability inspection

V

valid vote: Vote from a ballot or ballot image that is legally acceptable according to state law

validation: Process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements

verification: Process of evaluating a system or component to determine whether the products of a given development phase satisfy the conditions (such as specifications) imposed at the start of the phase

video ballot: Electronic voter interface which presents ballot information and voting instructions as video images. See also **ballot**.

vote for N of M: A ballot choice in which voters are allowed to vote for a specified number (“N”) of candidates in a multi-seat (“M”) contest

voted ballot: Ballot that contains all of a voter's selections and has been cast

voter verifiable: A voting system feature that provides the voter an opportunity to verify that his or her ballot selections are being recorded correctly, before the ballot is cast

voter verifiable audit record: Human-readable printed record of all of a voter’s selections presented to the voter to view and check for accuracy

voting equipment: All devices, including the voting machine, used to display the ballot, accept voter selections, record voter selections, and tabulate the votes

voting machine: The mechanical, electromechanical and electric components of a voting system that the voter uses to view the ballot, indicate their selections, verify their selections. In some instances, the voting machine also casts and tabulates the votes. See **voting equipment**.

voting officials: Term used to designate the group of people associated with elections, including election personnel, poll workers, ballot designers and those responsible for the installation, operation and maintenance of the voting systems.

voting position: Specific response field on a ballot where the voter indicates the selection of a candidate or ballot proposition response

voting station: The location within a polling place where voters may record their votes. A voting station includes the area, location, booth or enclosure where voting takes place as well as the voting machine. See **voting machine**.

voting system: The total combination of mechanical, electromechanical or electronic equipment (including the software, firmware, and documentation required to program, control, and support the equipment) that is used to define ballots; to cast and count votes; to report or display election results; and to maintain and produce any audit trail information; and the practices and associated documentation used to identify system components and versions of such components; to test the system during its development and maintenance; to maintain records of system errors and defects; to determine specific system changes to be made to a system after the initial qualification of the system; and to make available any materials to the voter (such as notices, instructions, forms or paper ballots).

voting system software: All the executable code and associated configuration files needed for the proper operation of the voting system. This includes third party software such as operating systems, drivers, and database management tools. See also **dynamic voting system software**, **semi-static voting system software**, and **static voting system software**.

voting system testing: Examination and testing of a computerized voting system by using test methods to determine if the system complies with the requirements in the *Voluntary Voting System Guidelines* and with its own specifications.

voting system test laboratory: Test laboratory accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) to be competent to test voting systems. When NVLAP has completed its evaluation of a test lab, the Director of NIST will forward a recommendation to the EAC for the completion of the accreditation process.

W

write-in voting: To make a selection of an individual not listed on the ballot. In some jurisdictions, voters may do this by using a marking device to physically write their choice on the ballot or they may use a keypad, touch screen or other electronic means to enter the name.

A.2 Sources

Definitions in this glossary are either extracted from or based on the following sources:

44 U.S.C. 35	United States Code, Title 44, Chapter 35, Information Security, Section 3542, Definitions.
ACM SIGCHI	ACM's Special Interest Group on Computer-Human Interaction, http://www.acm.org/sigchi/ (February 2005).
ADA	Americans with Disabilities Act of 1990.
ANSI Dictionary	American National Dictionary for Information Processing Systems, American National Standards Committee X3, Information Processing Systems, 1982.
ANSI 354	American National Standards Institute, International Committee for Information Technology Standards, Common Industry Format for Usability Test Reports, ANSI/INCITS 354-2001
ANSI C63.19	American National Standards for Methods of Measurement of Compatibility between Wireless Communications Devices and Hearing Aids, 2001.
electionline	http://electionline.org/ , (March 2005).

FIPS 81	Federal Information Processing Standard 81, DES Modes of Operations, December, 1980.
FIPS 140-2	Federal Information Processing Standard 140-2, Security Requirements for Cryptographic Modules, May 2001.
FIPS 199	Federal Information Processing Standard 199, Standards for Security Categorization of Federal Information and Information Systems, December 2003.
FIPS 201	Federal Information Processing Standard 201, Personal Identity Verification for Federal Employees and Contractors, February 2005.
HAVA	Help America Vote Act of 2002 - Public Law 107-252.
IEA	International Ergonomics Association, http://www.iea.cc/ , (February 2005).
IEEE 1583	IEEE P1583/D5.3.2 Draft Standard for the Evaluation of Voting Equipment, December 6, 2004.
ISO 5725	ISO/IEC 5725:1994 Accuracy (trueness and precision) of measurement methods and results.
ISO 9241	ISO/IEC 9241:1997 Ergonomic requirements for office work with visual display terminals (VDT).
ISO 17000	ISO/IEC 17000:2004 Conformity assessment -- Vocabulary and general principles.
ISO Guide 2-4	ISO/IEC Guide 2:2004 Standardization and related activities - General vocabulary.
ISO Guide 2-6	ISO/IEC Guide 2:1996 Standardization and related activities - General vocabulary.
NASS	National Association of Secretaries of State Election Reform Key Terms, http://www.nass.org/Election%20Reform%20Key%20Terms.pdf (February 2005).
NIST HB 143	NIST Handbook 143 State Weights and Measures Laboratories Program Handbook.
NIST HB 150	NIST Handbook 150:2001 NVLAP Procedures and General Requirements.
NIST HF Rpt.	NIST Special Publication 500-256 Improving the Usability and Accessibility of Voting Systems and Products, May 2004.

NIST SP 800-30	NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems, July 2002.
NIST SP 800-49	NIST Special Publication 800-49 Federal S/MIME V3 Client Profile, November 2002.
NIST SP 800-53	NIST Special Publication 800-53 Recommended Security Controls for Federal Information Systems, Appendix B, Glossary.
NIST SP 800-59	NIST Special Publication 800-59 Guideline for Identifying an Information System as a National Security System, August 2003.
NIST SP 800-63	NIST Special Publication 800-63 Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology, June 2004.
OMB A130	OMB Circular A-130, Appendix III.
Section 508 of the Rehabilitation Act of 1973, as amended.	Electronic and Information Technology Accessibility Standards (2002) Architectural and Transportation Barriers Compliance Board, 36 CFR Part 1194, http://www.accessboard.gov/sec508/508standards.htm .
Usability Glossary	Usability First Usability Glossary, http://www.usabilityfirst.com/glossary/main.cgi , (February 2005).
VIM	The ISO International Vocabulary of Basic and General Terms in Metrology (VIM), 1994.
VSS	2002 <i>Voting Systems Standards</i> , Volumes I and II. Federal Election Commission.
Whatis.com	http://Whatis.com , IT Encyclopedia

Appendix B: References

Table of Contents

B	References.....	B-3
B.1	Documents Incorporated in the <i>Guidelines</i>	B-3
B.2	Other Documents Used in Developing the Guidelines	B-5
B.3	Legislation References	B-6
B.4	Additional References	B-7

[Intentionally left blank]

Appendix B: References

B.1 Documents Incorporated in the *Guidelines*

The following publications have been incorporated into the Guidelines. When specific provisions from these publications have been incorporated, specific references are made in the body of the Guidelines.

Federal Regulations

Code of Federal Regulations, Title 29, Part 1910, Occupational Safety and Health Act

Code of Federal Regulations, Title 36, Part 1194, Architectural and Transportation Barriers Compliance Board, Electronic and Information Technology Standards - Final Rule

Code of Federal Regulations, Title 47, Parts 15 and 18, Rules and Regulations of the Federal Communications Commission

Code of Federal Regulations, Title 47, Part 15, “Radio Frequency Devices”, Subpart J, “Computing Devices”, Rules and Regulations of the Federal Communications Commission

American National Standards Institute (ANSI)

ANSI C63.4 Methods of Measurement of Radio-Noise Emissions from Low-Voltage Electrical and Electronic Equipment in the Range of 9Khz to 40 GHz

ANSI C63.19 American National Standard for Methods of Measurement of Compatibility between Wireless Communication Devices and Hearing Aids

ANSI-NCITS Industry Usability Reporting and the Common Industry Format
354-2001

International Electrotechnical Commission (IEC)

IEC 61000-4-2 Electromagnetic Compatibility (EMC) Part 4: Testing and Measurement Techniques. Section 2 Electrostatic Discharge Immunity Test (Basic EMC publication).

IEC 61000-4-3 Electromagnetic Compatibility (EMC) Part 4: Testing and Measurement Techniques. Section 3 Radiated Radio-Frequency Electromagnetic Field Immunity Test.

IEC 61000-4-4 (1995-01)	Electromagnetic Compatibility (EMC) Part 4: Testing and Measurement Techniques. Section 4 Electrical Fast Transient/Burst Immunity Test.
IEC 61000-4-5 (1995-02)	Electromagnetic Compatibility (EMC) Part 4: Testing and Measurement Techniques. Section 5 Surge Immunity Test.
IEC 61000-4-6 (1996-04)	Electromagnetic Compatibility (EMC) Part 4: Testing and Measurement Techniques. Section 6 Immunity to Conducted Disturbances Induced by Radio-Frequency Fields.
IEC 61000-4-8 (1993-06)	Electromagnetic Compatibility (EMC) Part 4: Testing and Measurement Techniques. Section 8 Power-Frequency Magnetic Field Immunity Test. (Basic EMC publication).
IEC 61000-4-11 (1994-06)	Electromagnetic Compatibility (EMC) Part 4: Testing and Measurement Techniques. Section 11. Voltage Dips, Short Interruptions and Voltage Variations Immunity Tests.
IEC 61000-5-7 Ed. 1.0 b:2001	Electromagnetic compatibility (EMC) Part 5-7: Installation and mitigation guidelines—Degrees of protection provided by enclosures against electromagnetic disturbances

National Institute of Standards and Technology

FIPS 140-2	Security Requirements for Cryptographic Modules
FIPS 180-2	Secure Hash Standard, August 2002
FIPS 186-2	Digital Signature Standard, February 2000
FIPS 188	Standard Security Label for Information Transfer
FIPS 196	Entity Authentication Using Public Key Cryptography
FIPS 197	Advanced Encryption Standard (AES)
SP 800-63	Electronic Authentication Guideline, Version 1.0.1

Military Standards

MIL-STD-498	Software Development and Documentation Standard, 1989
MIL-STD-810D(2)	Environmental Test Methods and Engineering Guidelines, 19 July 1983

B.2 Other Documents Used in Developing the Guidelines

The following publications have been used for guidance in the revision of the *Guidelines*.

American National Standards Institute (ANSI), International Organization for Standardization (ISO), International Electro-technical Commission (IEC)

ANSI/ISO/IEC TR 9294:1990	Information Technology Guidelines for the Management of Software Documentation
ISO/IEC TR 13335-4:2000	Information technology—Guidelines for the management of IT Security—Part 4: Selection of safeguards
ISO/IEC TR 13335-3:1998	Information technology—Guidelines for the management of IT Security—Part 3 Techniques for the management of IT security
ISO/IEC TR 13335-2:1997	Information technology—Guidelines for the management of IT Security—Part 2: Managing and planning IT security
ISO/IEC TR 13335-1:1996	Information technology—Guidelines for the management of IT Security—Part 1: Concepts and models for IT security
ISO 10007:1995	Quality Management Guidelines for Configuration Management
ISO 10005:1995	Quality Management Guidelines for Quality Plans
ANSI/ISO/ASQC QS9000-3:1997	QM and QA standards Part 3: Guidelines for the application of ANSI/ISO/ASQC Q9000-1994 to the Development, Supply, Installation, and Maintenance of Computer Software

Electronic Industries Alliance Standards

MB2, MB5, MB9	Maintainability Bulletins
EIA 157	Quality Bulletin
EIA QB2-QB5	Quality Bulletins
EIA RB9	Failure Mode and Effect Analysis, Revision 71
EIA SEB1—SEB4	Safety Engineering Bulletins
RS-232-C	Interface Between Data Terminal Equipment and Data Communications Equipment Employing Serial Binary Data Interchange
RS-366-A	Interface Between Data Terminal Equipment and Automatic Calling Equipment for Data Communication

RS-404 Standard for Start-Stop Signal Quality Between Data Terminal
Equipment and Non-synchronous Data Communication Equipment

National Institute of Standards and Technology

NISTIR 4909 Software Quality Assurance: Documentation and Reviews

Institute of Electrical and Electronics Engineers

610.12-1990 IEEE Standard Glossary of Software Engineering Terminology

730-1998 IEEE Standard for Software Quality Assurance Plans

828-1998 IEEE Standard for Software Configuration Management Plans

829-1998 IEEE Standard for Software Test Documentation

830-1998 IEEE Recommended Practice for Software Requirements
Specifications

Military Standards

MIL-STD-498 Software Development and Documentation, 27 May 1998

B.3 Legislation References

Help America Vote Act, Pub. L. 107-252, 42 USC Sections 15301-15545

Americans With Disabilities Act of 1990, Pub. L. 101-336, 42 USC Sections 12101-12213

42 USC 1974

Occupational Safety and Health Act, Pub. L. 91-596, 29 USC Sections 651-678, 42 USC
Section 3142-1

Architectural Barriers Act of 1968, Pub. L. 90-480, 42 USC Sections 4151-4157

Voting Rights Act of 1965, Pub. L. 89-110, 42 USC Sections 1973; 1973a-p; 1973aa;
1973aa-1-6; 1973bb; 1973bb-1

B.4 Additional References

The following publications contain information that is useful in understanding and complying with the *Guidelines*.

American National Standards Institute (ANSI), International Organization for Standardization (ISO), International Electro-technical Commission (IEC)

ANSI/ISO/IEC TR	Information Technology Guidelines for the Preparation of 10176.1998 Programming Language Standards
ANSI/ISO/IEC 6592.2000	Information Technology Guidelines for the Documentation of Computer Based Application Systems
ANSI/ISO/ASQC 1997	Quality management and quality assurance standards Part 3: Q9000-3- Guidelines for the application of ANSI/IAO/ASQC Q9001-1994 to the Development, supply, installation and maintenance of computer software
ANSI/ISO/ASQC Q9000-1-1994	Quality Management and Quality Assurance Standards—Guidelines for Selection and Use
ANSI/ISO/ASQC Q10007-1995	Quality Management Guidelines for Configuration Management
ANSI X9.31-1998	Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry, 1998
ANSI X9.62-1998	Public Key Cryptography for Financial Services Industry: The Elliptic Curve Digital Signature Algorithm, 1998
ISO/IEC 8:2001	ITU-T Recommendation X.509 (2000), Information technology - 9594- Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks

National Institute of Standards and Technology

FIPS 102	Guideline for Computer Security Certification and Accreditation
FIPS 112	Password Usage (3)
FIPS 113	Computer Data Authentication

Institute of Electrical and Electronics Engineers

488-1987	IEEE Standard Digital Interface for Programmable Instrumentation
796-1983	IEEE Standard Microcomputer System Bus IEEE/ANSI Software Engineering Standards
750.1-1995	IEEE Guide for Software Quality Assurance Planning
1008-1987	IEEE Standard for Software Unit Testing
1016-1998	IEEE Recommended Practice for Software Design Descriptions
1012-1998	IEEE Guide for Software Verification and Validation Plans

Military Standards

MIL-HDBK-454	Standard General Requirements for Electronic Equipment
MIL-HDBK-470	Maintainability Program for Systems & Equipment
MIL-HDBK-781A	Handbook for Reliability Test Methods, Plans, and Environments for Engineering, Development Qualification, and Production
MIL-STD-882	Systems Safety Program Requirements
MIL-STD-1472	<i>Human Engineering Design Criteria for Military Systems, Equipment and Facilities</i>
MIL-STD-973	Configuration Management, 30 September 2000

Other References

Designing for the Color-Challenged: A Challenge, by Thomas G. Wolfmaier (March 1999); http://www.sandia.gov/itg/newsletter/mar99/accessibility_color_challenged.html;

Effective Color Contrast: Designing for People with Partial Sight and Color Deficiencies, by Aries Arditi, Ph.D; http://www.lighthouse.org/color_contrast.htm

Electronic Markup Language (EML), Version 4.0, (Committee Draft) Organization for the Advancement of Structured Information Standards (OASIS), January 24, 2005

NIST Special Publication 500-256, Improving the Usability and Accessibility of Voting Systems and Products, <http://vote.nist.gov>

RSA Laboratories Technical Note, Public Key Cryptographic Standard (PKCS) #7: Cryptographic Message Syntax Standard, November 1, 1993

RSA Laboratories Technical Note, Extensions and Revisions to PKCS #7, May 13, 1997

The Americans with Disabilities Act Accessibility Guidelines (ADAAG 2202), Access Board; <http://www.access-board.gov/adaag/html/adaag.htm>

[Intentionally left blank]

Appendix C: Independent Verification Systems

Table of Contents

C	Independent Verification Systems	C-3
C.1	Independent Verification Systems	C-3
C.1.1	Improved Accuracy in Independent Verification Audits	C-3
C.1.2	Example Independent Verification Systems	C-4
C.1.2.1	The Split Process Architecture for IV Systems	C-5
C.1.2.2	End to End Cryptographic IV Systems.....	C-5
C.1.2.3	Witness IV Systems	C-6
C.1.2.4	Direct IV Systems.....	C-7
C.1.3	Handling Multiple Records Produced by IV Systems.....	C-8
C.2	Core Characteristics for Independent Verification Systems	C-9
C.3	Split Process Independent Verification Systems	C-10
C.3.1	Capture and Verification Stations	C-11
C.3.2	Data Formats for Token Objects	C-11
C.3.3	Storage and Communications of Records	C-12
C.4	Witness IV Systems	C-12
C.5	End to End Cryptographic IV Systems	C-13

[Intentionally left blank]

Appendix C: Independent Verification Systems

Appendix C is an informative section that describes Independent Verification systems followed by characteristics of the types of Independent Verification systems which will be used as the basis for future requirements. This information is preliminary and will be evolving with further research.

C.1 Independent Verification Systems

A primary objective for using electronic voting systems is the production of voting records that are highly precise, highly reliable, and easily counted - in essence, an accurate representation of ballot selections whose handling requirements are reasonable. To meet this objective, there are many factors to consider in an electronic voting system design, including:

- the environment provided for voting, including the physical and environmental factors
- the ease with which voters can use the voting system, i.e., its usability
- the robustness and reliability of the voting equipment
- the capability of the records to be used in audits

Independent Verification (IV) systems have as their primary objective the production of independent records of voter ballot selections that are capable of being used in audits in which their correctness can be audited to a very high level of precision. The primary voting security and integrity issues addressed by IV systems are:

- whether electronic voting systems are accurately recording ballot selections
- whether the ballot record contents can be audited precisely post-election

The threats addressed by IV systems are those that could cause a voting system to inaccurately record the voter's selections or cause damage to the voting system records. These threats could occur via any number of means including human error, accident or fraudulent activity. The threats are addressed mainly by providing, in the voting system design, the capability for ballot record audits to detect precisely whether specific records are correct as recorded or damaged, missing, or fraudulent.

C.1.1 Improved Accuracy in Independent Verification Audits

Independent Verification is the top-level categorization for electronic voting systems that produce multiple records of ballot selections that can be audited to a high level of precision. For this to happen, the records must be produced and made verifiable by the voter, and then subsequently handled according to the following protocol:

- At least two records of voter selections are produced and one of the records is then stored such that it cannot be modified by the voting system, e.g., the voting system creates a record of voter selections and then copies it to some unalterable media
- The voter must be able to verify that both records are correct, e.g., verify his or her selections on the voting system's display and also verify the second record of selections stored on the unalterable storage media
- The verification processes for the two records must be independent of each other and (a) at least one of the records must be verified directly by the voter, or (b) it is acceptable for the voter to indirectly verify both records if they are stored on independent systems
- The content of the two records can be checked later for consistency through the use of identifiers that allow the records to be linked

An assumption is made that at least one set of records is usable in an efficient counting process such as an automated tabulator, and the other set of records is usable in an efficient process of verifying its agreement with the other set of records used in the counting process. The sets of records would preferentially be different in form and thus have more resistance to accidental or deliberate damage.

Given these conditions, the multiple records are said to be distinct and independently verifiable; that is, both records are not under the control of the same processes. As a result of this independence, one record can be used to audit or check the accuracy of the other record. Because the storage of the records is separate, an attacker who can compromise one of the records still will face a difficult task in compromising the other.

C.1.2 Example Independent Verification Systems

The following sections present overviews of several types of IV systems. Some of these systems have not been marketed as yet but are included here to help clarify approaches to independent verification systems. The Independent Verification systems discussed are:

- voting systems with a split process architecture³
- end-to-end voting systems that include cryptographic audit schemes
- witness systems that take a picture of or otherwise capture an indirect verification of ballot selections
- direct independent verification, including voting systems that produce an optically scanned ballot or that produce a voter verifiable paper audit trail

³ The split process architecture is otherwise known as the frog protocol, which was first described in the Caltech – MIT report: *Voting: What Is, What Could Be*, as part of a modular voting architecture. The frog term, i.e., the token, was chosen specifically to convey no information about the physical form of the object used to carry vote information between two separate modules of the voting station. The report is available for download at <http://www.vote.caltech.edu/>.

C.1.2.1 The Split Process Architecture for IV Systems

A voting machine with a split process architecture consists of vote capture and verification stations that are separate, i.e., two physical devices. A voter inserts an object called a token into the capture station to make ballot selections and then takes the token object to the verification station to review and store his or her votes. The token object could be paper or unalterable media. Two records of the vote are created: one on the token object and one by the verification station. Either could be used in the final count.

For any split process voting system, the interaction between the voter and the split process operates as follows:

- A voter is given a token object that has been initialized to be blank
- Supporting information is written to the token object including the ballot and identification information about the election and precinct
- The voter inserts the token object into a capture station such as a DRE, which reads the ballot information from the token and then displays the ballot to the voter by some means such as a touch screen. The voter makes his or her ballot selections, which causes a record of the vote to be recorded on the token object
- The voter takes the token object to a separate verification station, which reads the recorded votes from the token object, makes an electronic copy, and displays it to the voter
- The voter verifies that the information is correct and then deposits the token object in a secure container so it can be archived and used later for recounts or audits against the electronic records

Two sets of records are produced: the electronic records and the token records. Typically, the electronic records recorded by the verification station would be counted in the election. The records should be different in form and be resistant to accidental or deliberate damage to be useful for audits and recounts.

In theory, the physical separation of vote capture from vote verification may make analysis of the capture and verification devices easier or less costly. The rationale is that the user interface software on the capture station is expected to be complex and difficult to verify for correctness. On the other hand, the verification station's software is expected to be less complicated because it need only copy the contents of the token, display it to the voter, and store the ballot selections. In general, segregating functions by placing them on physically different systems is a standard computer security practice for making those functions easier to test for correctness and easier to manage securely.

C.1.2.2 End to End Cryptographic IV Systems

End to end systems use cryptographic techniques to store an encrypted copy of the voter's ballot selections. In this way, ballot selections can be audited and demonstrated to have been included in the election count.

End to end systems in existence today generally operate as follows:

- A voter uses a voting machine such as a DRE to make ballot selections
- The DRE issues a paper receipt to the voter that contains information that permits the voter to verify that the choices were recorded correctly. The information does not permit the voter to reveal his or her selections
- The voter may have the option to check that his or her ballot selections were included in the election count, e.g., by checking a web site of values that (should) match the information on the voter's paper receipt

End to end systems are sometimes referred to as receipt-based systems. They may provide an assurance not only that the correct set of ballot choices was recorded, but that those selections were included in the election count. Some analyses of auditing and cryptographic systems assert that very small numbers of self-audits are required to verify the correctness of an election.

C.1.2.3 Witness IV Systems

A witness system creates the second record of ballot choices by using a separate module to record or witness the voter's verification of the first record. The primary feature of a witness system is that the creation of the record does not require action by the voter. This may result in quicker voting times or voting systems that are simpler to use than other approaches that involve multiple, direct verifications by the voter.

An example of a witness system is a DRE with a camera mounted above its screen. The camera takes pictures and saves them independently of the DRE. It would operate as follows:

- A voter makes ballot selections at the DRE and then presses a button to record his or her vote
- The DRE records the ballot selections and uses them in the election count
- At the time the button is pressed, the camera takes a picture of the DRE summary screen and saves the image. The voter would not be included in the picture.
- This collection of images constitutes a second ballot record that can be used in audits and recounts

As can be seen by this example, the voter's interactions are reduced to making ballot selections at the DRE and pressing a button to make the selections final. If the DRE were to be compromised such that it secretly recorded the ballot choices incorrectly, the stored photographic images would reflect what the voter had seen and verified at the DRE summary screen.

Because the voter may not be able to verify that the creation of the second record was performed accurately, it is important that the creation process be highly reliable and very

resistant to accidental or deliberate damage. Also, the suitability of the records for manual or automated auditing is a factor when considering this approach.

C.1.2.4 Direct IV Systems

Direct Independent Verification systems produce a record that the voter may verify directly with the voter's senses and which is then preserved for auditing or counting. Some optical scan voting systems fit this category, as well as DREs with VVPAT capability.

The optical scan voting systems in this category are those in which two records are created: a paper and an electronic record. This system uses Optical Scan Recognition (OCR) to create an electronic record from the paper record after the paper record has been directly verified by the voter. The general operation of this system is:

- A voter uses a marking device such as a DRE to mark a ballot and then presses a button to print the marked ballot
- The voter directly reviews the printed paper record to ensure its correctness, and if correct, places the paper record into a scanner. A procedure would be needed to handle voided ballots.
- The scanner converts the paper record into an electronic format. To reduce errors that may result from scanning the paper record, the paper records might contain a barcode representation of the human readable portion of the ballot.
- The paper record is deposited in a secure receptacle

No verification of the scanned paper record is performed in the above approach. One may assume that the scanning process is highly accurate and can be trusted to create the electronic record correctly; however it would be preferential for the voter to somehow verify that the record was, in fact, created correctly.

A DRE with VVPAT capability is similar to that of the optical scan above but consists typically of a DRE that both creates and records an electronic record, and a printer that creates a paper record of the voter's selections. Like the optical scan system, it creates two distinct representations of the voter's ballot selections: an electronic record and a paper record.

Typically, a voter would use the voting system as follows:

- A voter makes ballot selections and indicates that his or her selections are complete
- A paper record is printed of the voter's ballot selections as displayed on the summary screen. An alternative approach is to print the voter's ballot selections as they are made.
- The voter inspects and directly verifies that the paper record matches the displayed electronic record
- The paper record is deposited in a secure receptacle

Both approaches described here produce paper records that are verified directly by the voter through visual inspection. Voters with sight impairments would require an accessible device for verification that can produce an audible representation of the paper record.

C.1.3 Handling Multiple Records Produced by IV Systems

There are several fundamental questions that need to be addressed when designing the structure and selecting the physical characteristics of IV system records, including:

- how to tell if the records are authentic and not forged
- how to tell if the integrity of the records has remained intact from the time they were recorded
- the suitability of the records for various types of auditing
- how best to address problems if there are errors in the records

Whenever an electronic voting system produces multiple records of votes, there is some possibility that one or more of the records may not match. Records can be lost, or deliberately or accidentally damaged, or stolen, or fabricated. Keeping the two records in correspondence with each other can be made more or less difficult depending on the technologies used for the records and the procedures used to handle the records.

It is important to structure the records so that errors and other anomalies can be readily detected during audits. There are a number of techniques that can be used:

- associating unique identifiers with corresponding records, e.g., an individual paper record sharing a unique identifier with its corresponding electronic record
- including an identification of the specific voting system that produced the records, such as a serial number identifier, or by having the voting system digitally sign the records
- including other information about the election and the precinct or location where the records were created
- creating checksums of the electronic records and having the voting system digitally sign the entire sets of records so that missing or inserted records can be detected
- structuring the records in open, publicly documented formats that can be readily analyzed on different computing platforms

The ease with which records can be handled is a factor in the practical capability to conduct precise audits, given that some types of records are better suited to auditing and different voting environments than others. The factors that make certain types of records more suitable than others could vary greatly depending upon many other criteria, both objective and subjective. For example, paper records may require manual handling by poll workers and thus be more susceptible to accidental or deliberate damage, loss, and theft. At the same time, the extent to which the paper records must be handled will vary depending on the type of voting system in use. Electronic records may by their nature be more suitable for

automated audits; however electronic records are still subject to accidental or deliberate damage, loss, and theft.

C.2 Core Characteristics for Independent Verification Systems

This section contains a preliminary set of characteristics for IV systems. These characteristics are fundamental in nature and apply to all categories of IV systems. They will form the basis for future requirements for independent verification systems.

- A voting machine equipped with independent verification produces two independent records of ballot selections via interactions with the voter such that one record can be compared against the other to check their equality of content.

Discussion: This is the fundamental characteristic of IV systems. The records can be checked against one another to determine whether or not the voter's selections were correctly recorded.

- ◆ The voter verifies the content of each record and either (a) verifies at least one of the records directly or (b) verifies both records indirectly if the records are each under the control of independent processes.
- ◆ The creation, storage, and handling of the records are sufficiently separate such that the failure or compromise of one record does not cause the failure or compromise of another.

Discussion: The records must be stored on different media and handled independently of each other, so that no one process could compromise all records. If an attack can alter one record, it should still be very difficult to alter the other record.

- Both records are highly resistant to damage or alteration and should be capable of long-term storage.
- ◆ The records are linked to their corresponding records by including a unique identifier within each record that can be used to identify the corresponding record.
- ◆ The processes of verification for the multiple records do not all depend for their integrity on the same device or software module, and are sufficiently separate such that each record provides evidence of the voter's selections independently of the corresponding record.
- ◆ The records can be used in checks of one another, such that if one set of records can be used in an efficient counting process, the other set of records can be used for checking its agreement with the first set of records.

Discussion: For example, an electronic record can be used in an efficient counting process. A paper record can be used to verify the accuracy of the electronic

record. However, it is less suitable for efficient counting unless it can be corrected by an automated scan process.

- ◆ Each record includes an identification of the polling place and precinct.

Discussion: If the voting site and precinct are different, both should be included.

- ◆ The records include information identifying whether the balloting is provisional, early, or on election day, and information that identifies the ballot style in use.
- ◆ The records include a voting session identifier that is generated when the voting station is placed in voting mode and that can be used to identify the records as being created during that voting session.

Discussion: If there are several voting sessions on the same voting station on the same day, the voting session identifiers must be different. They should be generated from a random number generator.

- ◆ The records include a unique identifier associated with the voting station.

Discussion: The identifier could be a serial number or other unique ID.

- ◆ The cryptographic software in voting systems with independent verification is approved by the U.S. Government's Cryptographic Module Validation Program (CMVP) as applicable.

Discussion: Cryptographic software may be used for a number of different purposes, including calculating checksums, encrypting records, authentication, generating random numbers, and for digital signatures. This software should be reviewed and approved by the Cryptographic Module Validation Program. There may be cryptographic voting schemes where the cryptographic algorithms used are necessarily different from any algorithms that have approved CMVP implementations, thus CMVP approved software shall be used where feasible. The CMVP web site is <http://csrc.nist.gov/cryptval>.

C.3 Split Process Independent Verification Systems

This section contains characteristics specific to split process IV systems. The characteristics build on and are in addition to the core characteristics for IV systems. Split process systems consist of separate vote capture and verification stations, i.e., two physical devices. A voter inserts an object called a token into the capture station to make ballot selections and then takes the token object to the verification station to review and store his or her votes. Two records of the vote are created: one on the token object and one by the verification station.

C.3.1 Capture and Verification Stations

- The verification station is able to add information to the token object but cannot change prior recorded information.
- The capture and verification stations do not permit any communications between them except via the token object.
- The verification station shall log all rejected votes, including the precise contents of the votes and the identifier of the token object.

Discussion: The voter could reject and thereby void his or her ballot. This is to prevent the verification station from recording ballot selections that are different from what was entered at the capture station.

- The capture and verification stations could be purchased from different manufacturers and could use different operating systems.

Discussion: The greater the independence of the capture and verification stations, the less likely they could be compromised by the same threats, e.g., software viruses, or by a single conspiracy.

C.3.2 Data Formats for Token Objects

- The format for data written to the token object is specified and publicly available for use without licensing fees.
- The verification station verifies the correctness of the data on the token object and provides an indication of any errors to the voter.

Discussion: The verification station needs to verify that the data written to the token object was formatted properly according to the format specification and reject improperly formatted data. It also checks that the votes are consistent with the voting instructions, e.g., “vote for one, vote for two.”

- The record on the token object is digitally signed using a private key known only to the vote capture station and whose public key is distributed in an authenticated way to auditing systems and the verification station.
- The record created by the verification station is digitally signed using a private key known only to the verification station and whose public key is distributed in an authenticated way to auditing systems.
- The capture station associates a unique identifier with each record of voter selections to identify that record and link it to the corresponding record created by the verification station.

Discussion: The identifier serves the purpose of uniquely identifying the record to identify duplicates and/or for cross-checking two record types.

- The records from the verification station are randomly shuffled in memory when exported, so that the order of the records cannot be used to relate the votes to a specific voter.
- Rejected token objects are stored separately from accepted token objects for later auditing.

C.3.3 Storage and Communications of Records

- The verification station exports its records of voter choices accompanied by a digital signature on the entire set of electronic records and their associated digital signatures.

Discussion: This is necessary to determine if records are missing or substituted.

- The token objects are stored and transported in a physically secure way, using chain-of-custody mechanisms to ensure their integrity.
- The records from each station are randomly shuffled, so that an attacker learning the contents of those records at any point in the voting process can learn nothing about the order of votes cast.

C.4 Witness IV Systems

Witness IV systems are composed of two physically separate devices: the vote capture station that captures and stores records of voter selections, and the witness device that captures voter verifications of the records at the vote capture station. Because there are two devices, a number of the definitions for split verification systems apply equally well to witness systems. Because the vote capture station is in essence a DRE, a number of the definitions for DREs with VVPAT also apply to vote capture stations. A witness system fits somewhat loosely in the independent verification category because the voter performs only an indirect verification of ballot choices at the DRE. It is important that the witness device be tested extensively for accuracy and reliability and that malfunctions of the device be made immediately obvious to the voter and poll workers.

- A witness device records only a voter's verification at the vote capture station and stores the record so that it can be used for audit.
- A witness device acts as a passive device that cannot perform any operation with respect to the voting station other than to capture voter ballot selections as the voter verifies them.

Discussion: The witness device is synchronized with the voter verification of the ballot selections.

- A witness device, if attached to the vote capture station, is attached such that it can capture only the voter's verification of ballot selections.

Discussion: For example, the witness device could be connected only to the display unit and not the vote capture station's memory or disk drive.

- The vote capture station is able to detect whether the witness device is connected or in operation.

Discussion: If the witness device is not in operation, the vote capture station should cease recording voter selections.

- The vote capture station and the witness device are connected using a publicly available, published communications interface, such as RS232 or USB.
- Because voters must trust that the witness device records their verifications accurately, assessments of its software and functionality are straightforward, readily performed, and include extensive evaluation and penetration testing above and beyond what may be performed on voting systems that do not contain witness devices.

Discussion: Witness device manufacturers will be required to fully document their systems and conduct stringent testing.

- A voter should be able to inspect the record of his or her verification upon request.

Discussion: It is desirable that a voter have the ability to verify that the witness device is operating as specified.

- The witness device clearly indicates any malfunction in a way that is obvious to the voter and poll workers.
- The records captured by the witness device are able to be used in highly accurate verifications of the voting records of the voting station.
- The records contain unique identifiers that correspond to records stored by the vote capture station.
- The records are digitally signed by the witness device so that the integrity and authenticity of its records can be verified.
- A witness device is able to export its records in an open, nonproprietary format such that the records can be used in automated audits.
- The records are stored in the witness device and exported such that voter privacy is protected, e.g., by randomizing the order of the records.

C.5 End to End Cryptographic IV Systems

This section contains very preliminary definitions for end to end cryptographic-based IV systems. They are consistent with the characteristics of IV systems and build on the core characteristics of IV systems.

End to end voting systems use cryptographic mechanisms as a substitute for some physical, computer-security, or procedural mechanisms used to secure other types of voting systems. These cryptographic mechanisms can be used by a voter to verify that ballot selections were recorded correctly and counted in the election. Some auditing procedures normally performed by voting officials at the tabulation center can be done by voters or their designated representatives, using receipts issued by the voting system that work in conjunction with the cryptographic mechanisms. Typically, multiple individuals, known as designated trustees, hold key information that is combined to form encryption and decryption keys; thus, no one person is able to encrypt or decrypt. Several types of cryptographic voting approaches have been proposed or implemented, with varying properties. There are many cryptographic techniques (such as secure multiparty computation and homomorphic) that could be applied in novel ways in future voting systems.

- End to end systems record voters ballot selections at electronic voting machines and encrypt the records of votes for later counting by designated trustees.

Discussion: The voting station would operate much as a DRE.

- End to end systems produce a receipt that can be used by the voter in a process defined by voting officials that would enable the voter to verify that the voter's ballot selections were recorded correctly and counted in the election.

Discussion: The receipt could have a variety of different forms but likely would be printed on paper for the voter's ease of handling.

- No one designated trustee is able to decrypt the records; decryption of the records is performed by a process that involves multiple designated trustees.
- The receipt preserves voter privacy by not containing any information that can be used to show the voter's selections.
- The process used to verify that ballot selections were recorded correctly and counted preserves voter privacy by not revealing any information that can be used to identify the voter's selections.
- End to end systems store backup records of voter ballot selections that can be used in contingencies such as damage or loss of its counted records.

Discussion: This is necessary because the handling of the encrypted records requires the same chain of custody procedures as records produced by other voting systems and are thus subject to loss or damage. This could be paper for example.

- The backup records contain unique identifiers that correspond to unique identifiers in its counted records, and the backup records are digitally signed so that they can be verified for their authenticity and integrity in audits.

- Cryptographic software in end to end systems is documented thoroughly and subject to extensive verification testing for correctness. The documentation includes extensive discussion of how cryptographic keys are to be generated, distributed, managed, used, certified, and destroyed.
- Vote capture stations used in end to end systems must meet all the security, usability, and accessibility requirements.
- Reliability, usability, and accessibility requirements for printers in other voting systems apply as well to receipt printers used in end to end systems.
- Trustee systems are subject to the same evaluations and assessments as other voting systems.
- Systems for verifying that voter ballot selections were recorded properly and counted are implemented in a robust secure manner.

Discussion: Many of the cryptographic approaches have a "public append-only bulletin board" as a component; this is an important part of the system and needs to be implemented in a robust secure manner.

[Intentionally left blank]

Appendix D: Technical Guidance for Color, Contrast, and Text Size

Table of Contents

D	Technical Guidance for Color, Contrast, and Text Size	D-3
---	---	-----

[Intentionally left blank]

Appendix D: Technical Guidance for Color, Contrast, and Text Size

Although estimates vary, it is generally agreed that there are approximately 10 million visually impaired people in the United States. This estimate includes the 600,000 people who are legally blind. 8.1 million people were estimated to have a functional limitation in seeing in 1994, including both those with "non-severe limitation" (e.g., difficulty seeing words and letters) and those with "severe limitation" (e.g., unable to see words and letters). Approximately 1.8 million people in the U.S. have severe visual impairments but are not legally blind.⁴ Low vision includes dimness of vision, haziness, film over the eye, foggy vision, extreme near-sightedness or far-sightedness, distortion of vision, color distortion or blindness, visual field defects, spots before the eyes, tunnel vision, lack of peripheral vision, abnormal sensitivity to light or glare and night blindness. For the purposes of this discussion low vision is defined as having a visual acuity greater than 20/70.

People with low vision or color blindness will benefit from high contrast and selection of color combinations that are appropriate for their needs. Between 7% and 10% of all men have color vision deficiencies. Certain color combinations in particular cause problems. Therefore, use of color combinations with good contrast is required.

However, some users are very sensitive to very bright displays and cannot use them for long. An overly bright background causes a visual "white-out" which makes these users unable to distinguish individual letters. Contrast ratio between 6:1 and 15:1 is optimal.⁵

When color selection is provided the 16-color pallet as used in Microsoft Windows for 16 color displays and recognized by HTML 4.0 provides a sufficient range of both saturated and non-saturated color options. Use of non-saturated color options is an advantage for some people. The use of the 16-color palette or a larger color palette is suggested when voter adjustment of color is provided.

⁴ See the following sites for further detail:

<http://blue.census.gov/hhes/www/disable>

http://www.afb.org/info_document_view.asp?documentid=1367

<http://www.brailleinstitute.org>

⁵Cushman, W.H. and Rosenberg, D. J., Human Factors in Product Design. New York: Elsevier, 1991.

#	Color Name (Color names are per HTML 4.0)	RGB Value (Hexadecimal)
1	Black	#000000
2	Blue	#0000FF
3	Lime	#00FF00
4	Red	#FF0000
5	Aqua	#00FFFF
6	Fuchsia	#FF00FF
7	Yellow	#FFFF00
8	White	#FFFFFF
9	Navy	#000080
10	Green	#008000
11	Maroon	#800000
12	Teal	#008080
13	Purple	#800080
14	Olive	#808000
15	Grey	#808080
16	Silver	#C0C0C0

Large fonts provide significant help to users with low or impaired vision. A voting system is required to provide letters of at least 6.3 mm, for capital letters. A capital "X" is often used to make this measurement. It is not the size per se, but visual angle that is of primary importance. Visual angle is a measure, in degrees, of the size of the retinal image subtended by a viewed object. It represents the apparent size of an object based on the relationship between an object's distance from the viewer and its size (perpendicular to the viewer's line of sight). An object of constant size will subtend a smaller visual angle as it is moved farther from the viewer. Visual angle is typically defined in terms of minutes of visual arc. For people with normal vision, it is recommended that the height of characters in displayed text or labels be at least 16 minutes of arc (4.6 milliradians), and the preferred character height should be 22 minutes of arc (6.4 milliradians), which is preferred for reading tasks.

The size required for low vision accessibility is somewhat arbitrary, in that the larger the size the greater the number of low vision voters who can be accommodated. The Usability/Accessibility Task Group for IEEE P1583 recommends 30 minutes of arc, depending upon the presumed viewing distance. A table in the usability section of IEEE P1583 provides the following recommendations based on three possible viewing distances:

- for a distance of 51cm (20in): 4.43mm (.17in)
- for a distance of 64cm (25in): 5.54mm (.22in)
- for a distance of 76cm (30in): 6.65mm (.26in)

People with tunnel vision can only see a small part of the ballot at one time. For these users it is helpful to have letters at the lower end of the font size range in order to allow them to see more letters at the same time. Thus, there is a need to provide font sizes at both ends of the recommended range.

Use of sans serif fonts is also recommended for computer displays. Sans serif fonts have proven to be easier to read on computer screens than stylized fonts.

[Intentionally left blank]

EAC Commissioners

Chairman Paul DeGregorio

Vice Chairman Ray Martinez III

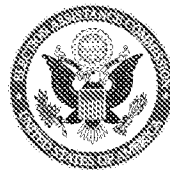
Commissioner Donetta Davidson

Commissioner Gracia Hillman

EAC Staff

Tom Wilkey, Executive Director

Juliet Thompson, General Counsel



U.S. Election Assistance Commission

1225 New York Avenue, NW

Suite 1100

Washington, DC 20005

866--747--1471 (toll free)

HAVAinfo@eac.gov

www.eac.gov

Electronic Patent Application Fee Transmittal

Application Number:	16745621			
Filing Date:	17-Jan-2020			
Title of Invention:	Optical Character Recognition Of Voter Selections For Cast Vote Records			
First Named Inventor/Applicant Name:	James M. Canter			
Filer:	Richard D. Egan/Marty Jones			
Attorney Docket Number:	HART:032C2			
Filed as Large Entity				
Filing Fees for Utility under 35 USC 111(a)				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
CLAIMS IN EXCESS OF 20	1202	2	100	200
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				200

Electronic Acknowledgement Receipt

EFS ID:	41468324
Application Number:	16745621
International Application Number:	
Confirmation Number:	6960
Title of Invention:	Optical Character Recognition Of Voter Selections For Cast Vote Records
First Named Inventor/Applicant Name:	James M. Canter
Customer Number:	36275
Filer:	Richard D. Egan/Marty Jones
Filer Authorized By:	Richard D. Egan
Attorney Docket Number:	HART:032C2
Receipt Date:	22-DEC-2020
Filing Date:	17-JAN-2020
Time Stamp:	16:56:54
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	\$200
RAM confirmation Number	E2020BLG57233475
Deposit Account	101205
Authorized User	Marty Jones

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

37 CFR 1.21 (Miscellaneous fees and charges)

37 CFR 1.20 (Post Issuance fees)

Ex. 2007 / PGR2025-00066 / Page 328 of 557

Election Systems & Software, LLC v. Hart Intercivic, Inc.

37 CFR 1.19 (Document supply fees)
37 CFR 1.17 (Patent application and reexamination processing fees)
37 CFR 1.16 (National application filing, search, and examination fees)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment/Req. Reconsideration-After Non-Final Reject	ROA032C2.pdf	436875	no	30
			cade9f7e3e3d5d2c43901bcd3ee90103ac90b5b2		
Warnings:					
Information:					
2	Amendment/Req. Reconsideration-After Non-Final Reject	Exhibit3.pdf	516404	no	9
			8e0b47c97597d725976c01043624d535e9065661		
Warnings:					
Information:					
3	Amendment/Req. Reconsideration-After Non-Final Reject	Exhibit1.pdf	656090	no	30
			85538deb3c865ab980ee96dcdc9e7d517dfb4dda		
Warnings:					
Information:					
4	Amendment/Req. Reconsideration-After Non-Final Reject	Exhibit2.pdf	1981636	no	228
			95597e0a95ab56dcae7f588fd71d0e41e512c367		
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	30126	no	2
			d3e918d47fed1a09d013ffd62af8ee4da88613fe		
Warnings:					
Information:					
Total Files Size (in bytes):			3621131		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: JAMES M. CANTER ET AL.

Filed: JANUARY 17, 2020

For: OPTICAL CHARACTER RECOGNITION OF VOTER SELECTIONS
FOR CAST VOTE RECORDS

Serial No.: 16/745,621

Group Art Unit: 2876

Examiner: GUDORF, L.

Atty Docket No.: HART:032C2

Electronically filed with the PTO

Commissioner For Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

**RESPONSE TO OFFICE ACTION DATED OCTOBER 5, 2020 AND EXAMINER
INTERVIEW SUMMARY**

This paper is submitted in response to the Office Action dated October 5, 2020. This paper also provides an Interview Summary of an Examiner Interview held December 8, 2020.

Amendments to the Claims

Please amend the claims as follows:

1. (Currently Amended) A method for electronic voting using printed vote records, comprising:

generating a printed vote record of at least one vote selection of a voter;

providing, on the printed vote record, voter readable text indicating the voter's at least one vote selection;

providing, on the printed vote record, encoded data, the encoded data based at least in part on the voter's at least one vote selection;

electronically scanning the voter readable text on the printed vote record to create a first data set, the first data set based at least in part on the voter's at least one vote selection;

electronically scanning the encoded data on the printed vote record to create a second data set, the second data set based at least in part on the voter's at least one vote selection;

comparing the first data set and the second data set; and

~~providing~~ generating a cast vote record indicating the voter's at least one vote selection, wherein, prior to generating the cast vote record, confirming an accuracy of the cast vote record one or more voter selections to be cast ~~confirmed~~ based at least in part on a comparison of the first data set and the second data set.

2. (Original) The method of claim 1, wherein the encoded data includes at least one bar code.

3. (Original) The method of claim 2, wherein the bar code is a one dimensional bar code.
4. (Currently Amended) The method of claim + 2, wherein the bar code is a two dimensional bar code.
5. (Currently Amended) The method of claim 4, wherein the two dimensional bar code is a Quick Response (QR) QR code bar code.
6. (Previously Presented) The method of claim 1, further comprising confirming an integrity of the printed vote record based at least in part on a comparison of the first data set and the second data set.
7. (Previously Presented) The method of claim 6, wherein confirming the integrity of the printed vote record comprises comparing the first data set to information provided in the encoded data.
8. (Previously Presented) The method of claim 7, wherein confirming the integrity of the printed vote record comprises comparing a first hash produced from the first data set to a second hash provided in the encoded data.
9. (Original) The method of claim 6, further comprising comparing the first data set to an election dictionary, the election dictionary containing at least potential vote choices.

10. (Original) The method of claim 9, wherein the comparing the first data set to an election dictionary is utilized to confirm the accuracy of an optical character recognition (OCR) process.

11. (Original) The method of claim 1, further comprising comparing the first data set to an election dictionary, the election dictionary containing at least potential vote choices.

12. (Previously Presented) The method of claim 11, wherein the comparing the first data set to an election dictionary is utilized to confirm the accuracy of an optical character recognition (OCR) process.

13. (Original) The method of claim 12, wherein the election dictionary contains at least one candidate name.

14. (Original) The method of claim 1, wherein the encoded data includes at least one bar code, bar code data of the bar code including data which is used to map the bar code to at least one particular vote selection.

15. (Previously Presented) The method of claim 14, wherein the at least one particular vote selection is a particular candidate.

16. (Previously Presented) The method of claim 14, wherein the data which is used to map the bar code to at least one particular vote selection is hash data.

17. (Previously Presented) The method of claim 14, wherein the bar code data of the bar code maps to the at least one particular vote selection through the use of a hash.

18. (Previously Presented) The method of claim 1, wherein the comparison of the first data set and the second data set is used to confirm that the at least one vote selection that the first data set is based at least in part on matches the at least one vote selection that the second data set is based at least in part on.

19. (Original) The method of claim 1, further comprising utilizing an election dictionary as part of the process to provide a cast vote record.

20. (Original) The method of claim 19, wherein the election dictionary includes at least a candidate name and other data affiliated with candidate name.

21. (Original) The method of claim 20, wherein the other data affiliated with a candidate name is a number.

22. (Original) The method of claim 21, wherein the number is a candidate sequence number or number indicative of a line of the printed vote record.

23. (New) The method of claim 1, further comprising confirming an accuracy of an optical character recognition (OCR) process by comparing a first hash produced from the first data set to a second hash provided in the encoded data.

24. (New) The method of claim 1, wherein the comparison of the first data set and the second data set is used to confirm an accuracy of an optical character recognition (OCR) process by confirming that the at least one vote selection that the first data set is based at least in part on matches the at least one vote selection that the second data set is based at least in part on.

REMARKS

Claims 1-24 are currently pending. Claims 23 and 24 are new dependent claims. Claim 1 is the sole independent claim.

Claim 5 is objected to. Office Action p. 2. Claim 5 has been amended as suggested in the Office Action.

Claim 4 is rejected under 35 USC 112 for an insufficient antecedent basis. Office Action p.2. Claim 4 has been amended to depend from claim 2 so as to correct the antecedent basis as suggested in the Office Action.

Claims 1, 2, 4-7, 14, 15 and 18 are rejected under 35 USC 102 based on Nadaf. Claim 3 is rejected under 35 USC 103 based on Nadaf in view of Brockhouse. Claims 8, 16, and 17 are rejected under 36 USC 103 based on Nadaf in view of Herskowitz. Claims 9-13, 16, and 19-22 are rejected under 36 USC 103 based on Nadaf in view of Heilper.

It is respectfully submitted that the Office Action has misinterpreted Nadaf.

Further, it is respectfully submitted that the translation of Nadaf relied upon in the Office Action has a mistranslation of one phrase (the translation was obtained from the Petitioner of a Post Grant Petition in a co-pending Post Grant Review of the parent patent (USP 10.445,966) of the pending application). Submitted herewith is the corrected Nadaf translation (“the Corrected Nadaf Translation”) as submitted by the Applicant in the pending Post Grant Review. Exhibit 1.¹

¹ For the purposes of this Response, it is respectfully asserted that the Nadaf reference and the combinations asserted fail to teach the claimed inventions irrespective of which translation is utilized. Appendix A at the end of this Response provides a more detailed explanation of the one error being pointed out in the translation.

This Response is structured as: (1) summarizing at a high level key differences between Nadaf and the independent claims, (2) briefly highlighting some of the aspects of the technology disclosed in the pending application, (3) providing a review of the Nadaf reference, (4) describing the distinctions between independent claim 1 and Nadaf, (5) describing additional elements of the dependent claims which distinguish the claims from the cited art, and (6) providing an examiner interview summary.

1. Summary of Nadaf Deficiencies

Nadaf provides a voting system with two main pieces of hardware described. Equipment 1 provides the equipment at which a voter votes and at which a cast vote record (CVR) is finalized and generated. This equipment provides the final CVR and such CVR is not changed. “After voting concludes,” the paper verification ballots 14 generated from equipment 1 are taken to some “other area” for post vote auditing by equipment 19. Equipment 1 which generates the CVR contains *no* optical character recognition (OCR) capability.

The sole independent claim describes the use of electronically scanning the voter readable text during the CVR generation process. Prior to generating the CVR, an accuracy of the data which generates the CVR is confirmed based at least in part on a comparison of an scanned text data set and a different scan (for example bar code scan) data set. In contrast, the CVR of Nadaf is generated without the use of scanning text and any OCR in Nadaf is merely described with regard to post-vote audit procedures after a CVR is finalized. Further, the claimed process helps to ensure the correctness of the process used to generate the CVR.

2. The Disclosed Technology

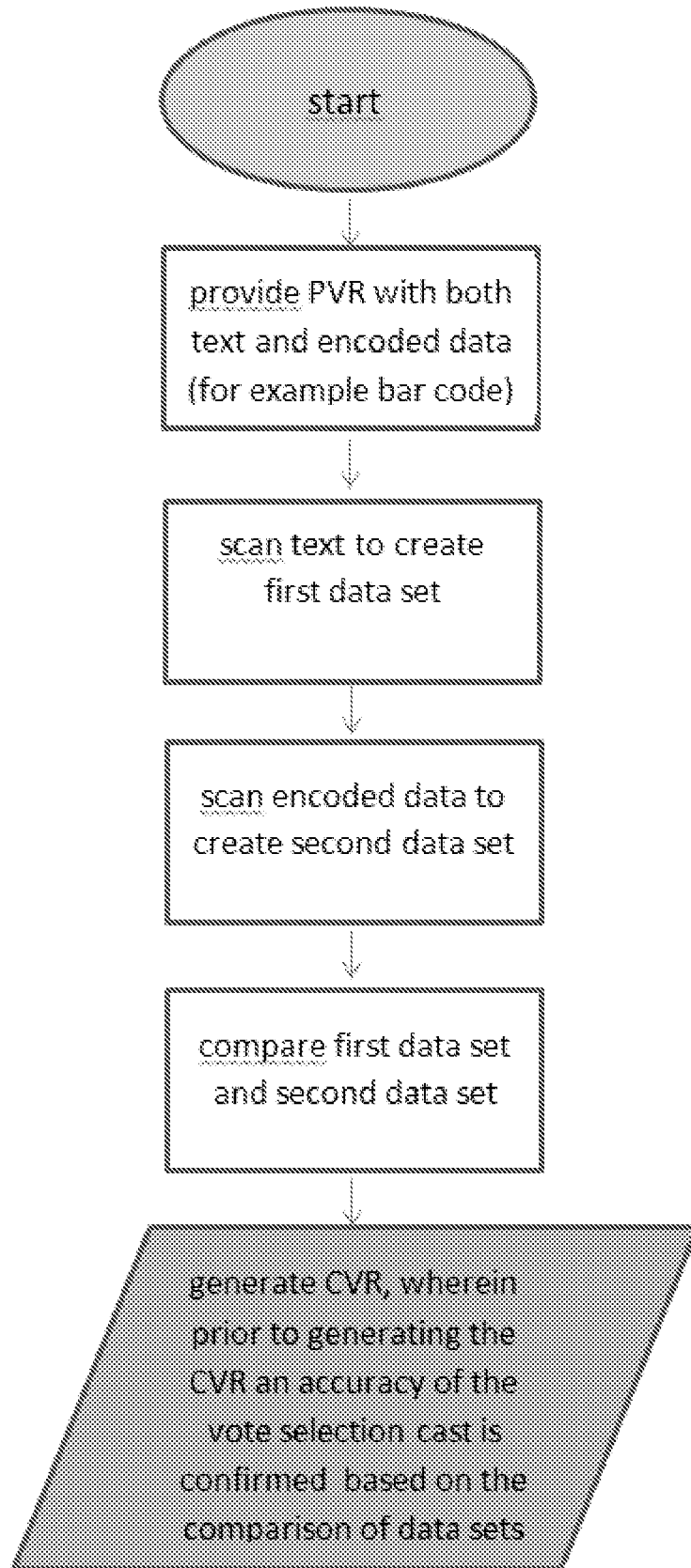
The pending application covers unique advances in optical character recognition (“OCR”) and error processing that allow electronic voting systems to interpret the voter-readable text (i.e., vote selections) on a printed ballot. This is in contrast with conventional systems that rely on bar codes to represent the vote selections on the ballots. One problem with such conventional systems is that voters cannot themselves verify the content of a bar code to ensure their vote is being accurately cast. Pending Application paragraph 0004. The Applicant’s claimed inventions in the pending application allow voters to have more confidence that their vote is being accurately counted because the system uses OCR to interpret the same printed text that a voter reads on the ballot.

Using OCR in the CVR process of a voting system is difficult because voting systems must be able to process an extremely high volume of records with an extremely high accuracy rate. For example, the 2005 Voluntary Voting System Guidelines published by the U.S. Election Assistance Commission requires that “the voting system shall achieve a target error rate of no more than one in 10,000,000 ballot positions, with a maximum acceptable error rate in the test process of one in 500,000 ballot positions.” Exhibit 2, p. 84. Indeed, as recently as April 2019, Election Systems & Software, LLC (the US market share leader in voting machines and the Petitioner in the Post Grant Review) asserted in a public letter to sitting U.S. Senators that no voting system could “use OCR to read [a candidate’s name] and record a vote reliably[.]” Exhibit 3, p. 6.

Through specific technical improvements, the inventions of the pending application achieve the required accuracy to use OCR in an electronic voting system. One specific technique described in the pending application is comparing the OCR results to encoded information (for example a bar code) printed on the printed vote record. Pending application, paragraph 0026. In some examples (and

in some claims of the pending application), the information in the encoded data / bar code may be a hash of the voter's original vote selections, which may be checked against a hash of the OCR results. Comparing the OCR results with information encoded in the bar code allows the system to confirm that the process for generating the CVR is accurate. Another technique described in the pending application is the use of an election dictionary. *Id.* at paragraph 0023. An election dictionary can include specific information relevant to the election (such as a list of candidate names, as well as additional information like the name of the specific contest). Checking the results of the OCR against this specialized election dictionary can help detect and correct errors from the OCR process. It is these innovations that allow the use of OCR on voter-readable voter selections as part of the process of creating a cast vote record. As discussed below, these innovations are not found in the prior art.

A flow chart providing a summary of the steps of independent claim 1 is provided below:



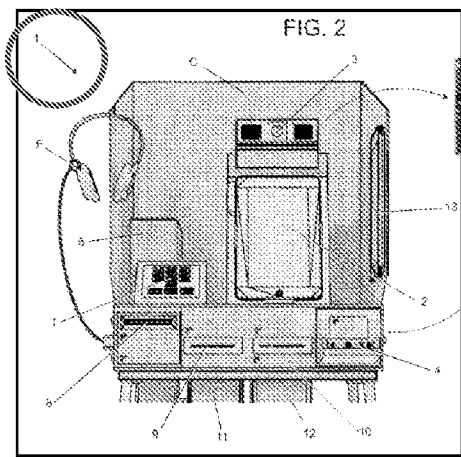
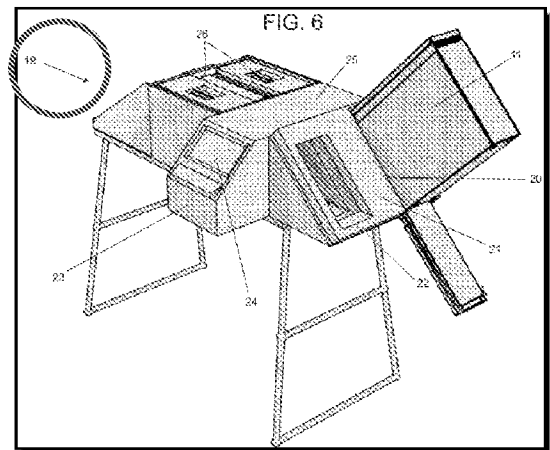
3. The Nadaf Reference

Nadaf is a Brazilian patent application. The original Nadaf reference is in Portuguese, and the Petitioner in the Post Grant Review provided a translation of Nadaf that was cited in the Office Action. As mentioned above, applicant has submitted a corrected Nadaf translation (“the Corrected Nadaf Translation”). Exhibit 1. The discussion of Nadaf as described herein is generally independent of which translation is utilized, except as particularly mentioned herein. To simplify this discussion, citations to Nadaf are made with respect to the Nadaf translation utilized by the Examiner.

Consistent with normal voting practices in Brazil, Nadaf discloses an electronic voting system that generates a digital record of the voter’s vote selections to effect the vote. Nadaf p. 15:13-15. (“Once the vote collection process is complete, the equipment (1) sends a digital signal to the electoral system to record the digital record of the vote[. . .]. In this manner, the vote is counted in a normal manner.”). Nadaf supplements the traditional direct-recording electronic (or “DRE”) system to address concerns with the Brazilian electronic voting system. Nadaf p. 7:9-13 (“scientific research [. . .] increasingly points to the need for the voter [. . .] to be able to verify that their voting intention was recorded and counted correctly without running the risk of faults caused by errors, which unfortunately are present *in fully electronic voting.*” (emphasis added)). Nadaf seeks to address these concerns by having the electronic voting device also generate a printed record of the electronic vote. Nadaf pp. 10:10-19 and 14:7-9. However, the printed record is not counted as the formal, legal vote; it merely “provid[es] the voter with assurance of their choice and prevent[s] equipment failure from being able to change the vote cast digitally.” Nadaf p. 10:18-11:1; Indeed, Nadaf emphasizes the historical problems with using paper ballots in Brazil to count votes. Nadaf p. 6:16-17 (“As is known historically, cultural trauma

has been caused by the period during which the country conducted its elections on paper ballots.”)

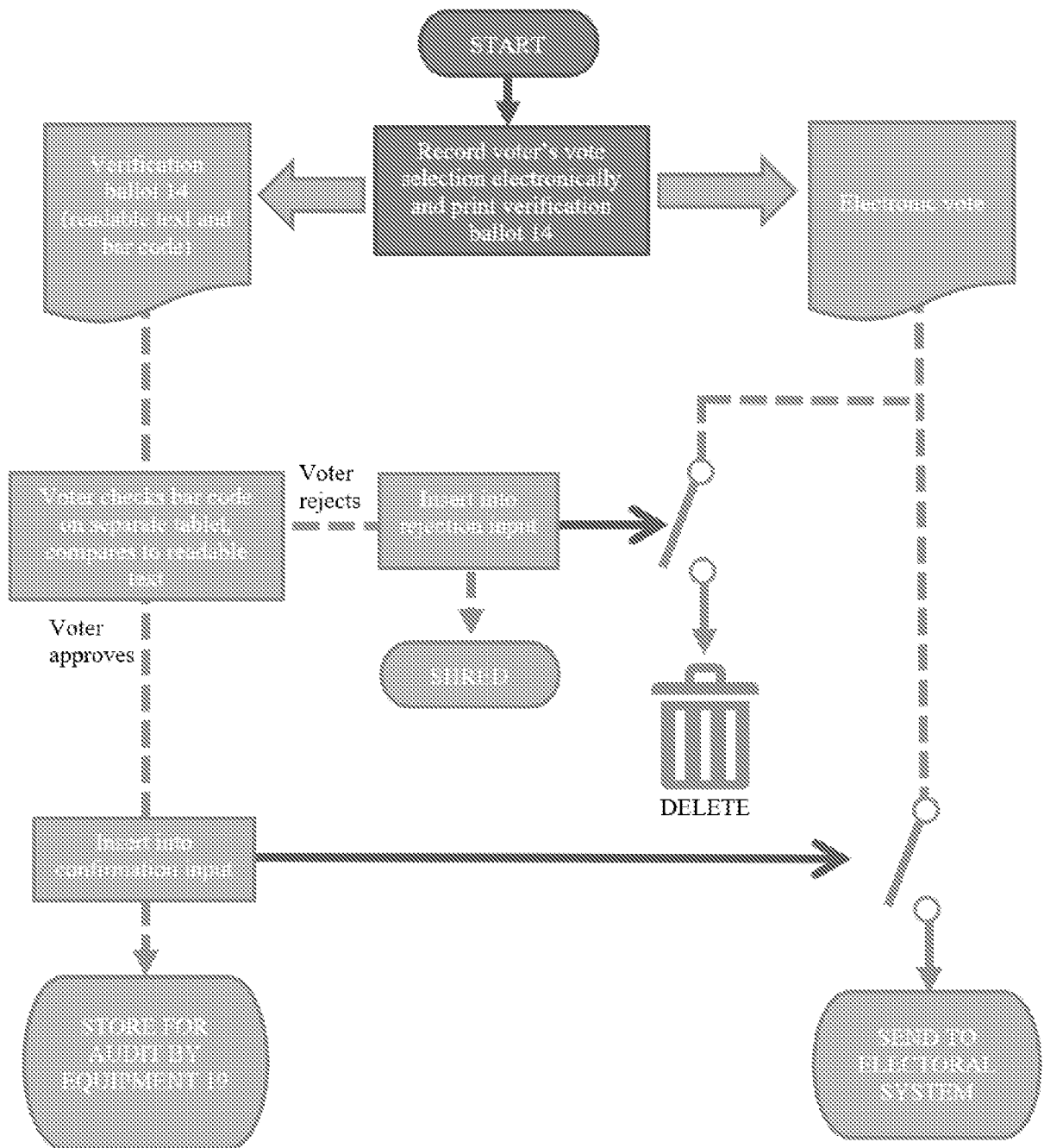
A critical aspect of Nadaf (one which the Post Grant Review Petitioner ignored) is its teaching that two distinct pieces of equipment are used for two distinct purposes. Nadaf p. 11:2-3. These are the “VERIFICATION BALLOT PRINTING AND COLLECTION EQUIPMENT” (equipment 1 in Figures 1, 2, and 3) and the “EQUIPMENT FOR AUDITING AND COUNTING VOTES PRINTED ON VERIFICATION BALLOTS” (equipment 19 in Figures 5, 6, and 7):



Nadaf p.11:4-18, p.26, and p. 29. Equipment 1 is used by the voter to cast a *digital* vote. Nadaf p. 15:13-15. Equipment 19, by contrast, is used—only after voting is complete and in a separate area—to audit paper records of the vote. Nadaf p. 17:13-18:3.

a) Equipment 1 generates electronic votes and paper records

The actual voting in Nadaf is all electronic and is handled exclusively by equipment 1. *See Nadaf* p. 13:10-12. Below is a flow chart summarizing the operations of equipment 1 in Nadaf:



The purpose of equipment 1 in Nadaf is to securely generate both an electronic vote and a paper verification ballot that can be used in later audits. The voter inputs his or her selections into equipment 1, which generates an electronic vote based on these selections. Nadaf p. 13:18-14:6. “Once collection of the electronic vote is complete, the voter authorizes [. . .] the printing of a verification ballot (14)” by printer output 8, which is part of equipment 1. Nadaf p. 14:7-9. The verification ballot 14 includes a text printout of the vote, various bar codes that contain digital signatures, and another bar code 15 that contains a complete copy of the voter’s vote selection. Nadaf p. 14:10-19.

The voter evaluates verification ballot 14, including using a separate tablet to decode the bar code 15 containing the voter’s selections. Nadaf p. 15:1-6. If the voter visually determines that verification ballot and decoded bar code are accurate, then the voter inserts verification ballot 14 into input device 9 to confirm the ballot. Nadaf p. 15:4-5. Equipment 1 recognizes the inserted ballot by scanning a *different* bar code, not bar code 15, containing verification information. Nadaf p. 15:6-7. Equipment 1 does not, however, scan any voter-readable text. Equipment 1 then “sends a digital signal to the electoral system to record the digital record of the vote[.]” Nadaf p. 15:13-15. This digital record of the vote is based on the previously-recorded electronic voter selection, not based on the scan of the verification ballot. Alternatively, if the voter visually determines that the verification ballot or decoded bar code do not match the voter’s intended selections, then the voter inserts ballot 14 into input 10 to reject the ballot. Nadaf p. 15:16-16:2. Inserting the ballot 14 into input 10 causes equipment 1 “to cancel the digital vote and relaunch the voter identification process, returning the entire voting process to the initial stage.” Nadaf p. 16:5-6.

Thus, in Nadaf, the printed ballot has no role in *generating* a separate electronic record of an individual voter's vote selections (whether by OCR scan or otherwise). Rather, verification ballot 14 is used by equipment 1 merely to release or delete the *existing* electronic vote. Nadaf p. 15:4-16:6. Importantly, equipment 1 of Nadaf does not have OCR capability and "record[s] the digital record of the vote" without ever using OCR. Nadaf p. 15:4-16:6. In Nadaf, OCR is performed (if at all) only as part of *auditing* steps performed by equipment 19 after voting is complete. *See* Nadaf p. 18:9-11.

b) Equipment 19 audits and counts paper records

"After voting concludes," the paper verification ballots 14 in collection urn 11 of equipment 1 are taken to some "other area" for auditing and counting by equipment 19. Nadaf p. 17:13-18:3. As indicated by its name, equipment 19 has two main functions: auditing verification ballots 14 and counting verification ballots 14. *See* Nadaf p. 5:16-6:14.

After confirming the integrity of collection urn 11, equipment 19 scans the verification ballots 14 using optical reader 25. Nadaf p. 19:1-9. At this point, equipment 19 also "compar[es] the text vote information to the vote information encoded into the bar code." Nadaf p. 19:8-9. Following this "comparative audit," equipment 19 performs another step that the Post Grant Review Petitioner translates as "the printed vote is then recorded electronically," but as noted in Appendix A, is more accurately translated as "the printed vote is then counted electronically" (from the original Portuguese: "o voto impresso é então contabilizado electronicamente"). *See* Nadaf p.19:10; Appendix A. Nadaf further states that equipment 19 will print "[r]eports, alerts and the total count bulletin [. . .] in text and two-dimensional bar code format;" these will also be retained "in the machine's print log." Nadaf p. 20:7-8.

Unlike equipment 1, equipment 19 does use OCR, but it does not generate anything that could qualify as a CVR with “voter selections [. . .] based on the voter readable text.” In fact, equipment 19 does not record any individual voter’s vote selections. It only provides a total, aggregate count of the previously created verification ballots 14, as a crosscheck on the original electronic voting.

4. Elements of independent claim 1 that the Office Action relies on to be in Nadaf that are missing from Nadaf

Claim 1 provides for scanning voter readable text to create a first data set and encoded data (for example a bar code) to create a second data set (elements 4 and 5 of the claim). Then a comparison of the two data sets is provided. Finally, a cast vote record (CVR) is generated in the last limitation. Further, prior to the generation of the CVR, an accuracy of the vote selection that is cast in the CVR is confirmed based at least in part on the comparison. It is noted that the final element has been amended to make clearer that the comparison is preformed prior to generating the CVR (as opposed to some later comparison after the CVR is generated). Thus, the last element now reads:

providing generating a cast vote record indicating the voter’s at least one vote selection, wherein, prior to generating the cast vote record, confirming an accuracy of the cast vote record one or more voter selections to be cast confirmed based at least in part on a comparison of the first data set and the second data set

Again it is noted that the first data set is an OCR-based data set obtained and utilized as part of the CVR generation process and the second data set is an encoded-based data set obtained and utilized as part of the CVR generation process.

It is respectfully asserted that Nadaf provides no teaching of creating the CVR using OCR or scanning text in any manner. As discussed above, the CVR of

Nadaf is generated and finalized in Equipment 1. OCR plays no role in such generation. It is noted that the Office Action cited Nadaf pages 15 lines 1-8 and 19 lines 7-12 for such limitations. However, it is respectfully noted that page 15 references equipment 1 and the only scan performed there is of the bar code. Nadaf p. 15:1-8. No OCR equipment is provided in equipment 1. As to the reference to page 19, that citation refers to Equipment 19 and the post vote auditing, a process done after the creation of the CVR. Equipment 19 does not provide, create, change, or modify a CVR in any way.

Further, independent claim 1 references comparing the first data set obtained from the scanned text and the second data set from the bar code scan to confirm the accuracy of the vote selection to be cast prior to generating the CVR. Nadaf does not teach having a scanned text data set and an encoded data set compared to confirm the accuracy of the vote selection cast in the CVR. As described above, this comparison process is one of the ways that the applicant's disclosure provides the high level of accuracy required to utilize OCR techniques when processing a CVR. As mentioned above, Nadaf does not use an OCR data set in the CVR process so Nadaf thus likewise does not compare a scanned text data set as part of the process to provide a cast vote record let alone confirm the accuracy of the data that yields the CVR based on such comparison.

It is respectfully asserted that Nadaf does not teach the limitations of claim 1. Thus, claim 1 and dependent claims 2-22 are patentably distinct from the cited art.

5. Additional elements of the dependent claims which distinguish the claims from the cited art

A. Election dictionary of dependent claims 9-13 and 19-22

As part of the process utilized with the first data set (the OCR data set used in the CVR process), various dependent claims recite the use of an election dictionary. For example, claim 9 (from which claim 10 depends) and Claim 11 (from which claims 12 and 13 depend) recite: “comparing the first data set to an election dictionary, the election dictionary containing at least potential vote choices.” Claim 19 (from which claims 20-22 depend) further recites: utilizing an election dictionary as part of the process to provide a cast vote record.

The Office Action combines Heilper to Nadaf and points to Heilper as teaching the claimed election dictionary. Office Action p.7-8. The pending claims at issue do not claim the generic use of just *any* dictionary to improve OCR in a voting system. Rather, the claims 9-13 require comparing the first data set to a specific kind of dictionary or utilizing a specific dictionary in the CVR process, an “*election* dictionary” and likewise claims 19-22 require the use of an “*election* dictionary as part of the process to provide a cast vote record,;

One way that the Applicant has solved the challenge of using OCR is by using a custom-tailored “election dictionary” in the OCR process. Pending Application paragraph 0007 (“[C]andidate names may be entered into the election dictionary and utilized for pattern matching to the OCR results.”). Matching OCR results against a defined election dictionary, which includes at least the candidate names on the ballot in a particular election, corrects many OCR errors without introducing new errors.

Heilper, in contrast, merely discloses a generic dictionary. Heilper never even mentions elections or vote choices, and a POSITA would understand that the recited election dictionary is meaningfully different from the dictionary of Heilper. The purpose of the election dictionary in the pending application is to “provide reliable matching of the OCR results with the proper ballot choice.” Pending application paragraph 0033. Simply applying a general-purpose dictionary to the

OCR used in a voting machine would not fulfill this purpose. Most voter selections will, of course, be proper nouns that do not appear in an ordinary dictionary. Using a specialized “election dictionary” it thus required. Attempting to match OCR results of candidates’ names to words in an ordinary dictionary could actually *increase* the errors in interpretation of the printed vote record.

Further, even if the claimed “election dictionary” and the particular details of the election dictionary provided in the claims is viewed as a species of the generic “dictionary” genus in Heilper, the combination still fails to make the claims obvious. Disclosure of a genus only renders the species obvious if the reference “describe[s] the genus containing those species such that a person of ordinary skill in the art would be able to envision every member of the class.” *Abbvie Inc. v. Mathilda & Terence Kennedy Inst. of Rheumatology Tr.*, 764 F.3d 1366, 1379 (Fed. Cir. 2014). Heilper does not meet this standard because a POSITA would not be able to envision from Heilper every possible specialized dictionary.

Moreover, there are elements of the election dictionary claims additionally not taught by the Nadaf and Heilper combination. For example dependent claims 9-13 require comparing the first data set (an OCR data) that is later used in the CVR process to an election dictionary. Likewise, dependent claim 19 recites utilizing the election dictionary as part of the process of providing a CVR. The mere combination of a generic dictionary does teach these specific uses of a dictionary.

In addition, there is no motivation to make the combination cited in the Office Action. A POSITA would not have believed that a generic dictionary as disclosed in Heilper would actually improve OCR for voting selections. Resolving the accuracy issues specific to voting (such as, for example, multiple candidates with similar names) requires an *election* dictionary as described in the pending

application. Adding the generic dictionary of Heilper would not solve this issue. In fact, using a generic dictionary in the voting system of Nadaf could create *more* errors in the interpretation of a printed vote record, making Nadaf unsatisfactory for its intended purpose. See *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 567 F.3d 1314, 1326-28 (Fed. Cir. 2009) (“Although predictability is a touchstone of obviousness, the ‘predictable result’ discussed in *KSR* refers not only to the expectation that prior art elements are capable of being physically combined, but also that the combination would have worked for its intended purpose”). Thus, because a POSITA would not predict that a *generic* dictionary would improve the operation of a *voting* system in Nadaf, this combination would not have been obvious to a POSITA.

Additionally, Federal Circuit precedent makes it clear that there is a requirement to show expectation of success that is separate from and additional to the requirement to show a motivation to combine. See *Cumberland Pharm. Inc. v. Mylan Institutional LLC*, 846 F.3d 1213, 1222 (“[The reasonable expectation of success requirement refers to the likelihood of success in combining references to meet the limitations of the claimed invention.]” (quoting *Intelligent Bio-Systems*, 821 F.3d at 1367)). Without modification, a generic dictionary would not be tailored to a particular election and would therefore not contain potential vote choices—which would almost exclusively be proper nouns. A POSITA would thus not expect success from adding “a dictionary” (as disclosed in Heilper) to the Nadaf system.

For these additional reasons it is respectfully asserted that dependent claims 9-13 and 19-22 are patentably distinct from the cited art.

**B. Claim for which an integrity of the printed vote record is confirmed
– claim 6 (and claims 7 and 8 which depend therefrom)**

Claim 6 (and claim 7 which depends therefrom) is rejected over Nadaf. Claim 8 (depending from claim 7) is rejected over Nadaf combined with Herskowitz. Claim 6 adds a printed vote record integrity limitation relating to confirming the integrity of a printed vote record utilizing OCR techniques: “confirming an integrity of the printed vote record based at least in part on a comparison of the first data set and the second data set.”

As described in the pending application, in addition to using OCR to create a CVR that includes the voter’s vote selection, the OCR process may be utilized to confirm the integrity of the printed vote record (PVR) itself (for example to establish that the PVR is a legitimate PVR and not has not been tampered with or altered). Pending application paragraph 0026. Thus, not only may the OCR be used to in the process of creating the CVR, the OCR may be used to confirm the integrity of the PVR.

The Office Action points to Nadaf page 6 lines 1-8 and page 19 lines 7-12, for the limitations related to confirming an integrity of a PVR. Office Action pp. 4-5. It is respectfully asserted that Nadaf does not teach the claimed integrity confirmation process.

Claim 6 (from which claims 7 and 8 depend) recites “confirming an integrity of the printed vote record based at least in part on a comparison of the first data set and the second data set.” It is noted again, that the first data set is the OCR data set utilized during the CVR process. It is respectfully noted that Nadaf page 6 line 1-8 does teach confirming the integrity of the printed vote record using a digital signature. However, it is noted that this passages references Equipment 19 (the audit equipment). The integrity confirmation does not relate to the comparison of the first and second data sets (the sets compared prior to casting the CVR). Rather, Nadaf describes verifying a digital signature for an integrity check but does not

describe comparing the two scans for that purpose. Rather, the scans are used for an audit counting purpose. As discussed above, Equipment 19 references audit activities performed after a cast vote record has been cast. Finally the passage at 19 lines 7-12 does describe OCR but such process is merely a comparative audit count of the printed vote records. No mention is made of establishing the integrity of a printed vote record (PVR) based on a comparison of the data sets used to generate the CVR. Nadaf does not teach comparing of data sets to establish an integrity of the PVR but at most only teaches comparisons of audit count results in the post vote equipment 19 and the use of digital signatures on the PVR.

As Nadaf provides no teaching of utilizing OCR of a PVR to establish the integrity of a PVR, let alone using the OCR data set that is utilized in the CVR process for such integrity check, it is respectfully that claims 6-8 are additionally distinct from the cited art for these reasons.

C. Claims including the use of a hash – claims 8 and 16-17

Dependent claims 8 and 16-17 are rejected over Nadaf in combination with Herskowitz. Each of these claims includes references to the use of hash techniques. Claim 8 recites:

wherein confirming the integrity of the printed vote record comprises comparing a first hash produced from the first data set to a second hash provided in the encoded data.

Claim 16 recites

wherein the data which is used to map the bar code to at least one particular vote selection is hash data.

Claim 17 recites

wherein the bar code data of the bar code maps to the at least one particular vote selection through the use of a hash.

The Office Action cites to Herskowitz for the hash limitations. Office Action pp 6-7.

One goal of Herskowitz is to “eliminate the need for [an] undesirable recount process.” Herskowitz 1:26-28. To achieve this goal, Herskowitz suggests allowing each voter to check “the voting precinct data processor” to confirm “that his vote was correctly recorded and not altered.” *Id.*, 1:63-67. Further, each voter is provided a receipt indicating the voter’s voting selections, which the voter could use to protest an allegedly incorrect electronic vote. *Id.*, 2:7-14. To deter false claims about incorrect electronic votes, Herskowitz teaches that a hash (in the form of an “EHT” or “encrypted hash total”) could be calculated from the electronic vote and then both stored in the data processor and printed on the voter’s receipt. *Id.* 1:48-58 and 2:1-7. Herskowitz further describes an optional process where all of the electronically stored EHTs in the data processor are recomputed and checked after the polls close. *Id.* 2:32-39. When a voter seeks to challenge an electronic vote record, the printed EHT can be compared against the electronically recorded EHT to detect any alteration made by the voter. *Id.*, 2:12-19.

i. claim 8

It is respectfully asserted that the cited combination does not perform the claimed comparison of hashes. Claim 8 requires “a first hash produced from the first data set to a second hash provided in the encoded data.” In claim 8, the first hash is produced from the first data set which (the OCR data set) and the second hash is produced from the second data set (the encoded data data set) is product as part of generating the first data set (“wherein generating the first data set further comprises generating an OCR hash”). Both claimed hashes are thus obtained from information on the printed vote record (e.g., from the readable text and from the barcode). The combination cited in the Office Action does not disclose (1) the

recited OCR hash / first hash (from OCR) or (2) a comparison of two hashes obtained from the printed vote record. More specifically, Herskowitz does not disclose a first hash produced from a data set created by OCR or the comparison of two hashes from the printed vote record. *See* Herskowitz, 3, Fig. 2 and 1:44-58 (hash calculated electronically from electronic voter selections and printed on receipt). Thus, merely adding the hash value procedures of Herskowitz to the method of Nadaf would not achieve the claimed methods. Substantial modifications would also be required.

First, the combination would still lack an OCR-derived hash. The digital signatures in Nadaf, and the bar codes in which the digital signatures are printed on the ballot, are not generated using OCR. *See* Nadaf p. 14 (describing bar codes with digital signatures from “the Election Judge” and “another entity auditing the process”). Thus, adding the hash of Herskowitz to Nadaf would lack the claimed “OCR hash” or the “first hash” that is produced from the data set created utilizing optical character recognition (OCR) on the scanned voter readable text.”

Second Herskowitz does not disclose a comparison of two hashes that are both obtained from information on the printed vote record. Instead, the comparisons in Herskowitz always involve at least one hash stored in electronic form. Herskowitz, 2:7-12 (“the administrator would scan the VIN on the receipt to access the allegedly recorded vote [. . .] in the data processor and the computer program would compare the recorded EHT with the EHT on the receipt.”).

ii. claims 16 and 17

As to claims 16 and 17, these claims relate to mapping a bar code to a vote selection through the use of a hash (claim 6: “wherein the data which is used to map the bar code to at least one particular vote selection is hash data” and claim 7: “wherein the bar code data of the bar code maps to the at least one particular vote selection through the use of a hash”). Herskowitz does not disclosure the use of a

hash in conjunction with a bar code. Rather, the hash is merely a hash of an electronic record created from the electronic vote as stored in the computing system. Specifically, the hash in Herskowitz is a hash (in the form of an “EHT” or “encrypted hash total”) that is calculated from the electronic vote and then both stored in the data processor and printed on the voter’s receipt. *Id.* 1:48-58 and 2:1-7. What is printed on the voter’s receipt is merely the results of this hash, the alphanumeric result “XXX...XXX” shown at the bottom of Herskowitz Figure 6. *Id.* 3:28-30 and Figure 6. Herskowitz makes no mention of providing a hash in conjunction with bar code and the combination likewise does not provide such a teaching.

It is thus respectfully asserted that the hash limitations of claims 8 and 16-17 provide additional distinctions from the cited art which independently establish patentability of these claims.

D. New Claims 22-23

New claims 22 and 23 provide additional details relating to a comparison of the first data set and the second data set. Both claims provide techniques for improving an OCR process. In claim 23, the improvement is provided by comparing a first hash produced from the first data set to a second hash provided in the encoded data. In claim 24, the improvement is provided by confirming that the at least one vote selection that the first data set is based at least in part on matches the at least one vote selection that the second data set is based at least in part on. It is respectfully assert that none of the cited prior art singularly or in combination teaches improving the accuracy of an OCR process by comparisons related to data sets utilized in generating a CVR.

6. Interview Summary

The applicant thanks Examiner Gudorf for conducting a telephonic interview with applicant's counsel, Richard Egan, and co-inventor James Canter. The interview was conducted on December 8th. Background as to the problem addressed by the pending application was discussed along with how the method flow of independent claim 1 addresses such problems. The teachings of the disclosure of Nadaf were also discussed. Applicant's counsel indicated that arguments for patentability of the claims in comparison to Nadaf would be presented in the written Response.

CONCLUSION

Please charge \$200.00 for two additional dependent claims. Should any additional fees under 37 CFR 1.16-1.21 be required for any reason relating to the enclosed materials, the Commissioner is authorized to deduct such fees from Deposit Account No. 10-1205/HART:032C2. The examiner is invited to contact the undersigned at the phone number indicated below with any questions or comments, or to otherwise facilitate expeditious and compact prosecution of the application.

Respectfully submitted,

/Richard D. Egan/
Richard D. Egan
Registration No.: 36,788
Attorney for Applicant

EGAN, PETERMAN, ENDERS & HUSTON, LLP
1101 South Capital of Texas Highway
Building C, Suite 200
Austin, Texas 78746
(512) 347-1611
FAX: (512) 347-1615

APPENDIX A

Though not needed for Applicant's arguments and not relied upon in the Response to Office Action, applicant notes that the translation utilized by the Office Action (Petitioner's translation from the PGR) translates the original Portuguese: "o voto impresso é então contabilizado electronicamente" (Nadaf p. 19:10) as "the printed vote is then recorded electronically." However a more accurate translation is "the printed vote is then counted electronically" Such an interpretation conforms to the counting purpose of equipment 19 ("EQUIPMENT FOR AUDITING AND *COUNTING* VOTES PRINTED ON VERIFICATION BALLOTS"—*counts* the printed verification ballots. Nadaf, pp. 5:7-10, 11:14-18, 19:1-2, 20-3-4) (emphasis added).

Further, with regard to "o voto impresso é então contabilizado electronicamente," the proper definition of "conta" (the root of "contabilizado") is a "sum," or "account." Thus, the excerpt the PGR Petitioner relies on should be translated as "the printed vote is then counted electronically," which is consistent with equipment 19 outputting a "total count bulletin." Nadaf p. 20:6-7.

That "counted" is the correct translation of "contabilizado" is confirmed by the fact that elsewhere in Nadaf, the PGR Petitioner translated related words ("contabilidade" and "contabilizada") as "count," such as translating "auditoria e contabilidade de votos impressos" as "audit and *count* the votes printed" (Nadaf p. 20:3-6 (emphasis added)) and translating "intenção de voto foi registrada e *contabilizada* corretamente" as "voting intention was recorded and *counted* correctly" (Nadaf p. 7:11-12(emphasis added)). The PGR Petitioner translation of the phrase "intenção de voto foi registrada e contabilizada corretamente" from Nadaf's background section is particularly telling, because there, the PGR Petitioner translated "contabilizada" as "counted" and translated a different word

(“registrada”) to mean “recorded.” Nadaf 7:11-12. And the PRG Petitioner’s translation of similar background discussion of equipment 19 further confirms the mistranslated Portuguese word “contabilizado.” Specifically, while the PGR Petitioner translated the action (“contabilizado”) as “recorded,” it translated the related modifier (“contabilidade”) describing the system performing that action as “counting.” Compare Nadaf, 6:7-9 (translation: “a simplified vote counting system”) with original: “sistema simplificado de contabilidade de votos.” A POSITA reading the original Nadaf reference would understand that the “simplified counting system” of equipment 19—which Nadaf calls the “EQUIPMENT FOR AUDITING AND COUNTING VOTES PRINTED ON VERIFICATION BALLOTS”—counts the printed verification ballots.

This interpretation of Nadaf is further confirmed by other statements in the same paragraph of the passage in question as that paragraph describes the post-audit step as “*counting* of all the votes” and “electronic tabulating of the printed ballots.” Nadaf p. 19:10-15. Further, Nadaf clarifies that “[f]or security purposes,” equipment 19 has specific, limited features: it “has only the disk storing the programs to control the mechatronic motors and to interpret, audit and *count* the votes printed.” Nadaf p. 20:3-6 (emphasis added).

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875				Application or Docket Number 16/745,621		Filing Date 01/17/2020		☐ To be Mailed		
ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO										
APPLICATION AS FILED - PART I										
		(Column 1)	(Column 2)							
FOR		NUMBER FILED	NUMBER EXTRA	RATE (\$)		FEE (\$)				
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))		N/A	N/A	N/A						
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))		N/A	N/A	N/A						
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))		N/A	N/A	N/A						
TOTAL CLAIMS (37 CFR 1.16(i))		minus 20 =	*	x \$100 =						
INDEPENDENT CLAIMS (37 CFR 1.16(h))		minus 3 =	*	x \$460 =						
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))		If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).								
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))										
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL						
APPLICATION AS AMENDED - PART II										
		(Column 1)	(Column 2)	(Column 3)						
AMENDMENT	12/22/2020	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)		ADDITIONAL FEE (\$)		
	Total (37 CFR 1.16(i))	* 24	Minus	** 22	= 2	x \$100 =		200		
	Independent (37 CFR 1.16(h))	* 1	Minus	*** 3	= 0	x \$480 =		0		
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
						TOTAL ADD'L FEE		200		
		(Column 1)	(Column 2)	(Column 3)						
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)		ADDITIONAL FEE (\$)		
	Total (37 CFR 1.16(i))	*	Minus	**	=	x \$0 =				
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x \$0 =				
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
						TOTAL ADD'L FEE				
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.						SLIE				
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".						/JASON ANTHONY JORDAN/				
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".										
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.										

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/745,621	01/17/2020	James M. Canter	HART:032C2	6960
36275	7590	12/14/2020	EXAMINER	
Egan, Peterman, Enders & Huston LLP.			GUDORF, LAURA A	
1101 S. Capital of Texas Highway			ART UNIT	
Bldg C, Suite 200			PAPER NUMBER	
Austin, TX 78746			2876	
			NOTIFICATION DATE	DELIVERY MODE
			12/14/2020	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

epehadmin@ipaustin.com
mjones@ipaustin.com

<i>Applicant-Initiated Interview Summary</i>	Application No. 16/745,621	Applicant(s) Canter et al.	
	Examiner LAURA A GUDORF	Art Unit 2876	AIA (FITF) Status Yes

All participants (applicant, applicants representative, PTO personnel):

(1) Laura Gudorf.

(3) Jim Canter.

(2) Rich Egan.

(4) ____.

Date of Interview: 08 December 2020.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.

If Yes, brief description: ____.

Issues Discussed ☐101 ☐112 ☒102 ☐103 ☐Others

(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: 1.

Identification of prior art discussed: NADAF.

Substance of Interview

(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Applicant and Examiner discussed differences between the instant invention and the prior art. No agreement was reached..

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☒ Attachment

/LAURA A GUDORF/
Primary Examiner, Art Unit 2876

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record

A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) 1.133 Interviews

Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.

All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiners responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicants correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:

- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:

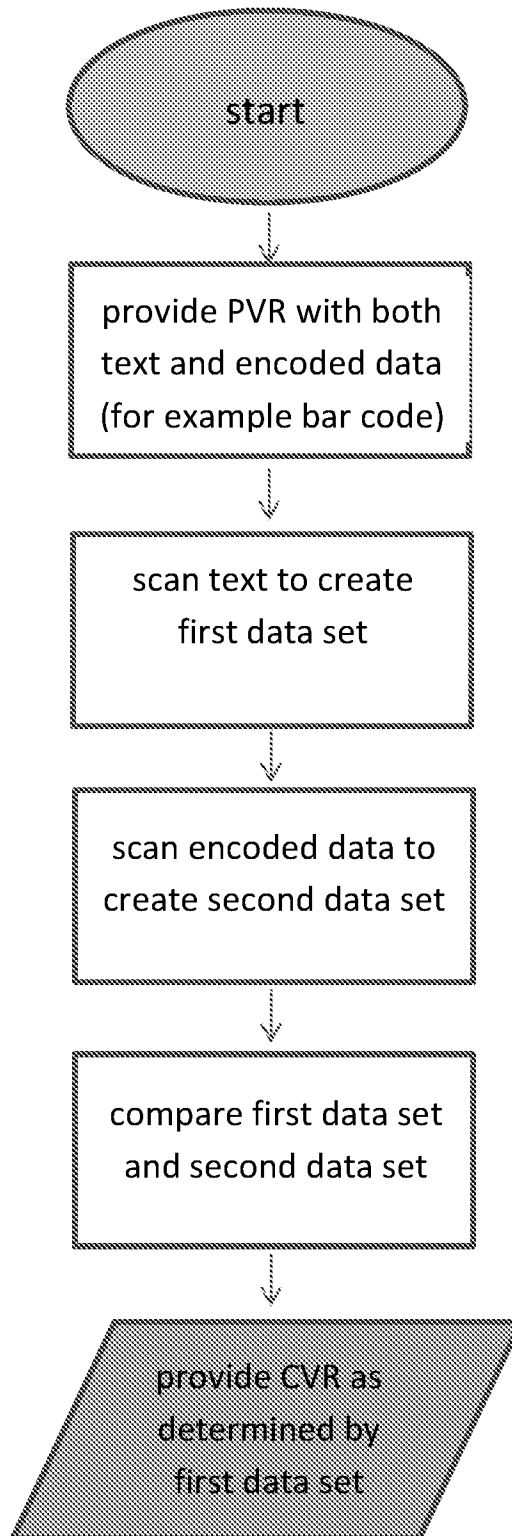
- 1) A brief description of the nature of any exhibit shown or any demonstration conducted,-
- 2) an identification of the claims discussed,
- 3) an identification of the specific prior art discussed,
- 4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
- 5) a brief identification of the general thrust of the principal arguments presented to the examiner,
(The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
- 6) a general indication of any other pertinent matters discussed, and
- 7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicants record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

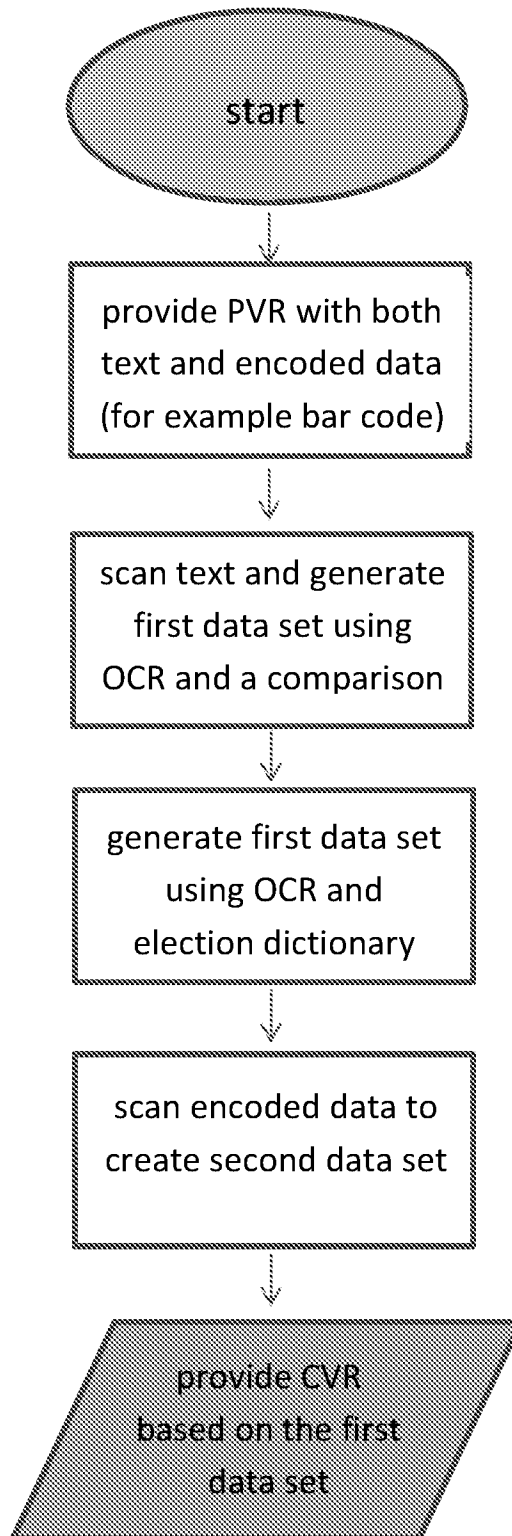
Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiners version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, Interview Record OK on the paper recording the substance of the interview along with the date and the examiners initials.

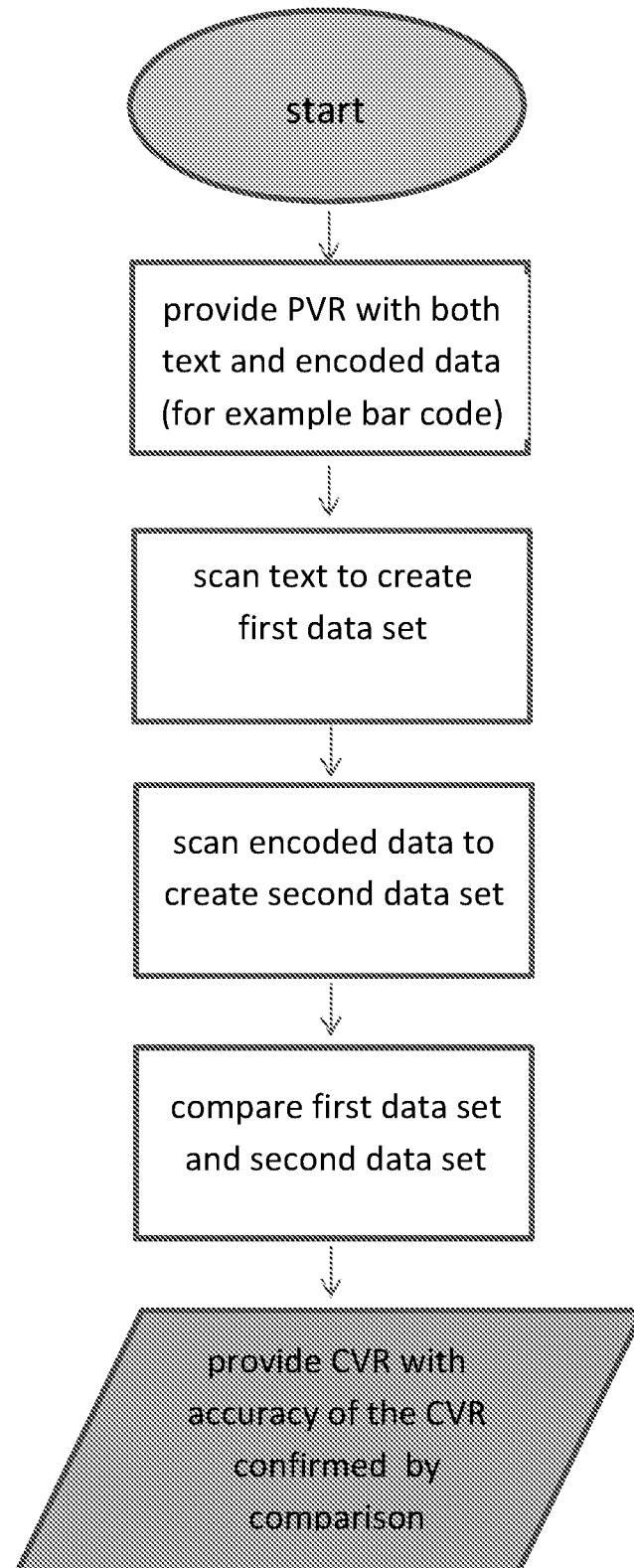
Application 16/919,267 (Atty Ref HART:032C3)
HIGH LEVEL CLAIM 1 FLOW (not all limitations listed)



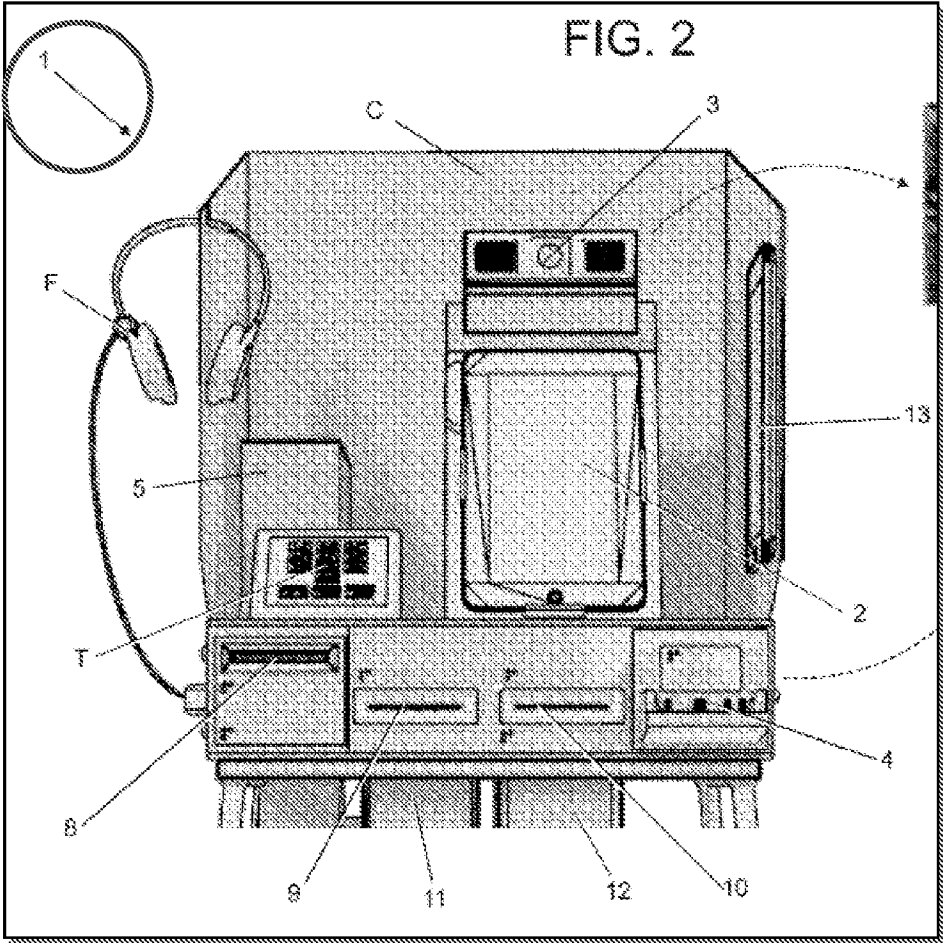
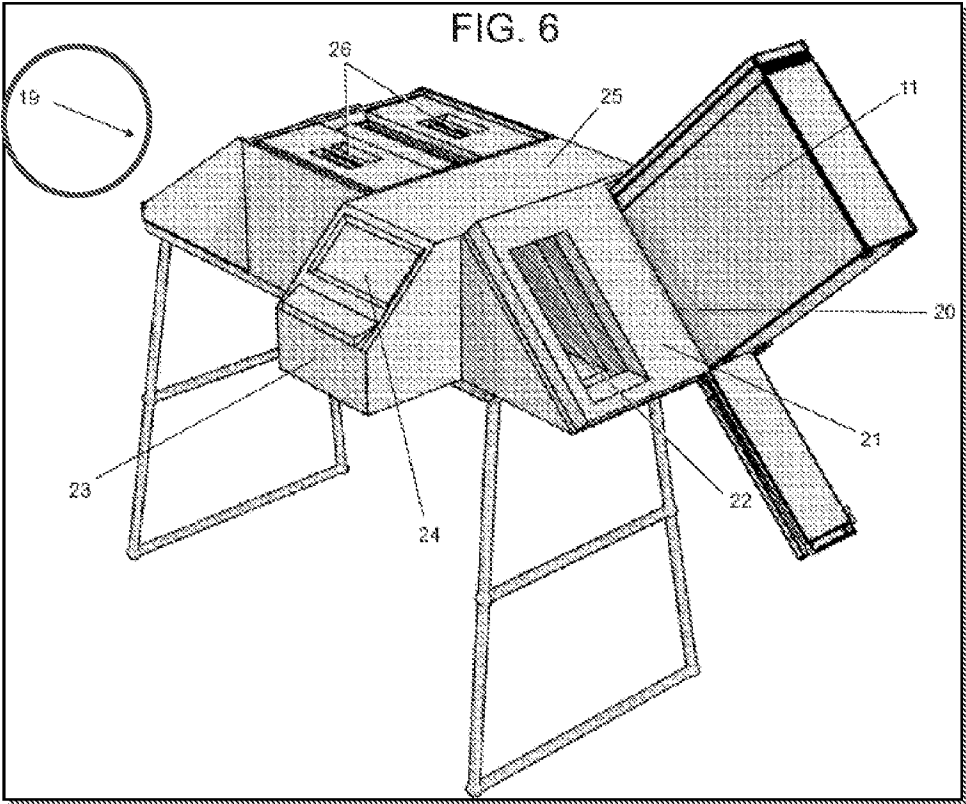
Application 16/919,267 (Atty Ref HART:032C3)
HIGH LEVEL CLAIM 18 FLOW (not all limitations listed)

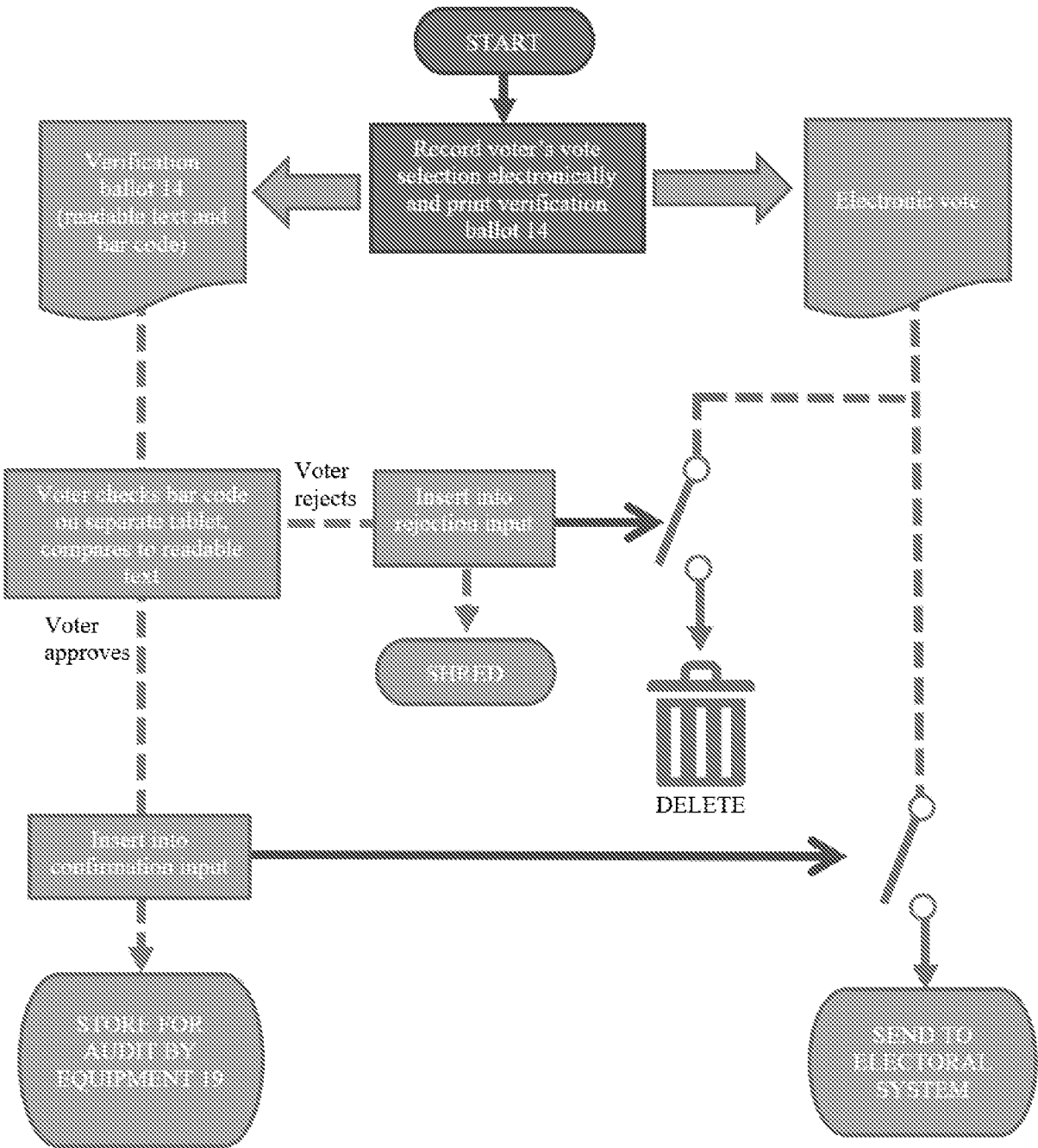


Application 16/745,621 (Atty Ref HART:032C2)
HIGH LEVEL CLAIM 1 FLOW (not all limitations listed)



Equipment 1 - "VERIFICATION BALLOT PRINTING AND COLLECTION EQUIPMENT"
Equipment 19 - "EQUIPMENT FOR AUDITING AND COUNTING VOTES PRINTED ON VERIFICATION BALLOT"





INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		16745621
	Filing Date		2020-01-17
	First Named Inventor	JAMES M. CANTER	
	Art Unit		
	Examiner Name		
	Attorney Docket Number		HART:032C2

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

Add

U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20060282442		2006-12-14	Lennon et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button.

Add

FOREIGN PATENT DOCUMENTS							Remove	
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²ⁱ	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button

Add

NON-PATENT LITERATURE DOCUMENTS			Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		16745621
	Filing Date		2020-01-17
	First Named Inventor	JAMES M. CANTER	
	Art Unit		
	Examiner Name		
	Attorney Docket Number	HART:032C2	

1	
---	--

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16745621
Filing Date	2020-01-17
First Named Inventor	JAMES M. CANTER
Art Unit	
Examiner Name	
Attorney Docket Number	HART:032C2

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Richard D. Egan/	Date (YYYY-MM-DD)	2020-11-30
Name/Print	Richard D. Egan	Registration Number	36788

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	41247313
Application Number:	16745621
International Application Number:	
Confirmation Number:	6960
Title of Invention:	Optical Character Recognition Of Voter Selections For Cast Vote Records
First Named Inventor/Applicant Name:	James M. Canter
Customer Number:	36275
Filer:	Richard D. Egan/Marty Jones
Filer Authorized By:	Richard D. Egan
Attorney Docket Number:	HART:032C2
Receipt Date:	30-NOV-2020
Filing Date:	17-JAN-2020
Time Stamp:	15:27:10
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	IDS.pdf	1034941	no	4
			0507ac8a3d161edbe73415dc62bfb6d2be6b46e4		

Warnings:

Information:	
Total Files Size (in bytes):	1034941
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>	

UNITED STATES PATENT AND TRADEMARK OFFICE
COMMISSIONER FOR PATENTS
P.O.BOX 1450
ALEXANDRIA VA 22313-1451

PRESORTED
FIRST-CLASS MAIL
U.S. POSTAGE PAID
POSTEDIGITAL
NNNNN

Egan, Peterman, Enders & Huston LLP.
1101 S. Capital of Texas Highway
Bldg C, Suite 200
Austin, TX 78746



**Courtesy Reminder for
Application Serial No: 16/745,621**

Attorney Docket No: HART:032C2

Customer Number: 36275

Date of Electronic Notification: 10/05/2020

This is a courtesy reminder that new correspondence is available for this application. If you have not done so already, please review the correspondence. The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

An email notification regarding the correspondence was sent to the following email address(es) associated with your customer number:

epehadmin@ipaustin.com
mjones@ipaustin.com

To view your correspondence online or update your email addresses, please visit us anytime at **<https://ppair-my.uspto.gov/pair/PrivatePair>**.

If you have any questions, please email the Electronic Business Center (EBC) at EBC@uspto.gov or call 1-866-217-9197.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/745,621	01/17/2020	James M. Canter	HART:032C2	6960
36275	7590	10/05/2020	EXAMINER	
Egan, Peterman, Enders & Huston LLP.			GUDORF, LAURA A	
1101 S. Capital of Texas Highway			ART UNIT	
Bldg C, Suite 200			PAPER NUMBER	
Austin, TX 78746			2876	
			NOTIFICATION DATE	DELIVERY MODE
			10/05/2020	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

epehadmin@ipaustin.com
mjones@ipaustin.com

Office Action Summary

Application No.

16/745,621

Applicant(s)

Canter et al.

Examiner

LAURA A GUDORF

Art Unit

2876

AIA (FITF) Status

Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on 09/22/2020.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on ____.

2a) ☐ This action is **FINAL**.

2b) ☒ This action is non-final.

3) ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on ____; the restriction requirement and election have been incorporated into this action.

4) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☒ Claim(s) 1-22 is/are pending in the application.

5a) Of the above claim(s) ____ is/are withdrawn from consideration.

6) ☐ Claim(s) ____ is/are allowed.

7) ☒ Claim(s) 1-22 is/are rejected.

8) ☐ Claim(s) ____ is/are objected to.

9) ☐ Claim(s) ____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10) ☐ The specification is objected to by the Examiner.

11) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a) ☐ All b) ☐ Some** c) ☐ None of the:

1. ☐ Certified copies of the priority documents have been received.

2. ☐ Certified copies of the priority documents have been received in Application No. ____.

3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

3) ☐ Interview Summary (PTO-413)

Paper No(s)/Mail Date ____.

2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b)

4) ☐ Other: ____.

Paper No(s)/Mail Date 01/28/2020; 03/17/2020; 03/20/2020; 09/14/2020;
09/21/2020

Ex. 2007 / PGR2025-00066 / Page 378 of 557

DETAILED ACTION

Summary

The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

This is a first Office Action on the merits.

Claims 1-22 are currently pending.

Claim Objections

Claim 5 is objected to because of the following informalities:

In claim 5, lines 1-2, please amend “the two dimensional bar code is a QR code bar code” to recite “the two dimensional bar code is a Quick Response (QR) code”;

Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of 35 U.S.C. 112(b):

(b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 4 recites the limitation "the bar code" in line 1. There is insufficient antecedent basis for this limitation in the claim. In particular, claim 4 recites dependency to claim 1 which does not recite “a bar code”. For purposes of examination, claim 4 has been interpreted as depending from claim 2 for proper antecedent basis.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a)(1) the claimed invention was patented, described in a printed publication, or in public use, on sale, or otherwise available to the public before the effective filing date of the claimed invention.

(a)(2) the claimed invention was described in a patent issued under section 151, or in an application for patent published or deemed published under section 122(b), in which the patent or application, as the case may be, names another inventor and was effectively filed before the effective filing date of the claimed invention.

Claim(s) 1, 2, 4-7, 14, 15, and 18 is/are rejected under 35 U.S.C. 102(a)(1) and 102(a)(2) as being anticipated by NADAF, BR102013018558 (Certified Translation).

Re claim 1:

NADAF teaches a method for electronic voting using printed vote records, comprising:

Generating a printed vote record of at least one vote selection of a voter (page 14, lines 7-9);

Providing, on the printed vote record, voter readable text indicating the voter's at least one vote selection (page 14, lines 10-14);

Providing, on the printed vote record, encoded data, the encoded data based at least in part on the voter's at least one vote selection (page 14, lines 10-14);

Electronically scanning the voter readable text on the printed vote record to create a first data set, the first data set based at least in part on the voter's at least one vote selection (page 15, lines 1-8; page 19, lines 7-12);

Electronically scanning the encoded data on the printed vote record to create a second data set, the second data set based at least in part on the voter's at least one vote selection (i.e., the verification ballot printing and collection equipment includes an OCR reading device, wherein the verification ballot printing and collection equipment recognizes voter readable text (page 15, lines 1-8; page 18, lines 4-11; page 19, lines 7-12));

Comparing the first data set and the second data set (page 15, lines 1-8; page 19, lines 7-12); and

Providing a cast vote record indicating the voter's at least one vote selection, an accuracy of the cast vote record confirmed based at least in part on a comparison of the first data set and the second data set (page 19, lines 7-12).

Re claim 2:

NADAF teaches the method of claim 1, wherein the encoded data includes at least one bar code (page 10, lines 11-12; Figure 4).

Re claim 4:

NADAF teaches the method of claim 2, wherein the bar code is a two dimensional bar code (page 10, lines 11-12; Figure 4).

Re claim 5:

NADAF teaches the method of claim 4, wherein the two dimensional bar code is a QR code (Figure 4).

Re claims 6-7:

NADAF teaches the method of claim 1, further comprising confirming an integrity of the printed vote record based at least in part on a comparison of the first data set and

the second data set (page 6, lines 1-8; pages 19, lines 7-12); wherein confirming the integrity of the printed cote record comprises comparing the first data set to information provided in the encoded data (page 6, lines 1-8; pages 19, lines 7-12)).

Re claim 14:

NADAF teaches the method of claim 1, wherein the encode data includes at least one barcode, barcode data of the barcode including data which is used to map the barcode to at least one particular vote selection (page 14, lines 10-14).

Re claim 15:

NADAF teaches the method of claim 1, wherein the at least one particular vote selection is a particular candidate (Figure 4).

Re claim 18:

NADAF teaches the method of claim 1, wherein the comparison of the first data set and the second data set is used to confirm that the at least one vote selection indicated by the first data set matches the at least one vote selection indicated by the second data set (page 6, lines 1-8; pages 19, lines 7-12).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103 which forms the basis for all obviousness rejections set forth in this Office action:

A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

Claim 3 is/are rejected under 35 U.S.C. 103 as being unpatentable over NADAF, BR 102013018558 in view of BROCKHOUSE, US 2014/0231513.

Re claim 3:

NADAF teaches the method of claim 2, but does not state that the barcode is a one dimensional barcode.

BROCKHOUSE teaches providing encoded data indicating the voter's at least vote in a one dimensional barcode (vote selection barcodes 112 [0106] [Figure 6]).

It would have been obvious to one of ordinary skill in the art before the effective filing date for the encoded data to include a one-dimensional barcode for the purpose of providing an alternative encoding medium.

Claims 8, 16, and 17 is/are rejected under 35 U.S.C. 103 as being unpatentable over NADAF, BR 102013018558 in view of HERSKOWITZ, US 6,971,574.

Re claims 8, 16, and 17:

NADAF teaches the method of claims 1 and 7, as discussed above, wherein the encoded data (barcode) stores digital signatures of the election judge and other auditing institutes (page 5, lines 5-158; page 6, lines 2-10).

NADAF does not confirming the integrity of the printed vote record comprises comparing a first hash produced from the first data set to a second hash provided in the encoded data; wherein the data which is used to map the barcode to at least one vote selection is hash data.

HERSKOWITZ teaches an electronic voting system which assigns confidential hash numbers to ballot choices (paragraph 1, lines 44-48). The system totals the corresponding hash numbers to produce a hash value for the voter (paragraph 1, lines 52-67). The hash value is further encrypted to produce an encrypted hash total (EHT). The EHT is stored in memory and is further printed on the voter's receipt. The first hash (recorded hash) and the second hash (printed EHT) are provided on the printed vote record and compared to verify the integrity of the printed vote (column 2, lines 12-17).

It would have been obvious to one of ordinary skill in the art before the effective filing date to further incorporate additional hash value procedures to further increase the security of NADAF's voting method by providing an additional way to verify the vote (column 2, lines 12-17).

Claims 9-13, 16, and 19-22 is/are rejected under 35 U.S.C. 103 as being unpatentable over NADAF, BR102013018558 in view of HEILPER, US 7,406,201.

Re claims 9-13 and 19-22:

NADAF teaches wherein the voter readable text further comprises at least a candidate name and other data affiliated with the candidate name [Figure 4]; the other data affiliated with a candidate name is a number, wherein the number is indicative of a line of the printed vote record or indicative of a candidate sequence number [Figure 4].

NADAF does not teach comparing the first data set to an election dictionary; wherein comparing the first data set to an election dictionary confirms the accuracy of an OCR process.

HEILPER teaches generating a data set from human readable text using OCR and compares the data set to a dictionary (directory of known strings) for OCR error correction (column 3, lines 15-35; column 5, lines 10-22; Figure 2); wherein the comparing the first data set to a dictionary is utilized to confirm an accuracy of an OCR process (column 3, lines 15-35; column 5, lines 10-22; Figure 2).

It would have been obvious to one of ordinary skill in the art before the effective filing date to further incorporate the aforementioned teachings of HEILPER in the method of NADAF such that the first data set is compared to a dictionary for the purpose of identifying and correcting OCR errors (column 5, lines 10-22).

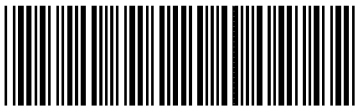
Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LAURA A GUDORF whose telephone number is (571)270-7607. If the Examiner cannot be reached by telephone, she can be reached through the following e-mail address: laura.gudorf@uspto.gov. The examiner can normally be reached on M-F 6:00-4:00 PM.

If attempts to reach the examiner by telephone and e-mail are unsuccessful, the examiner's supervisor, Michael Lee can be reached on (571)272-2398. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/LAURA A GUDORF/
Primary Examiner, Art Unit 2876

<i>Search Notes</i> 	Application/Control No. 16/745,621	Applicant(s)/Patent Under Reexamination Canter et al.
	Examiner LAURA A GUDORF	Art Unit 2876

CPC - Searched*		
Symbol	Date	Examiner
G07C13/00; G06K7/10346; G06K9/00442; G06K17/0032	09/22/2020	LAG

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
Inventor name search	09/22/2020	LAG
EAST - see attached search history	09/22/2020	LAG
PGR2020-00031 Reviewed Petition for Post Grant Review of U.S. Patent 10,445,966 on 09/21/2020	09/22/2020	LAG

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

	Ex. 2007 / PGR2025-00066 / Page 387 of 557
--	--

<i>Index of Claims</i> 	Application/Control No. 16/745,621	Applicant(s)/Patent Under Reexamination Canter et al.
	Examiner LAURA A GUDORF	Art Unit 2876

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS										
☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47										
CLAIM		DATE								
Final	Original	09/29/2020								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								
	21	✓								
	22	✓								

Doc code: IDS

PTO/SB/08a (03-15)

Doc description: Information Disclosure Statement (IDS) Filed

Approved for use through 07/31/2016. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)

Application Number	16745621
Filing Date	2020-01-17
First Named Inventor	JAMES M. CANTER
Art Unit	
Examiner Name	
Attorney Docket Number	HART:032C2

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	7635088		2009-12-22	Kevin Chung et al.	
	2	7988047		2011-08-02	Kevin Chung et al.	
	3	8261986		2012-09-11	Kevin Chung et al.	
	4	8991701		2015-03-31	Steve Bolton et al.	
	5	5497318		1996-03-05	Takayoshi Miyagawa et al.	
	6	10445966		2019-10-15	Canter et al.	
If you wish to add additional U.S. Patent citation information please click the Add button.						Add
U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)

Application Number	16745621
Filing Date	2020-01-17
First Named Inventor	JAMES M. CANTER
Art Unit	
Examiner Name	
Attorney Docket Number	HART:032C2

1	20090289115	2009-11-26	Kevin Chung et al.
2	20180350180	2018-12-06	Daniel Onischuk
3	20170344538	2017-11-30	Hiroya Horai
4	20140231513	2014-08-21	Sean Brockhouse et al.
5	20020084325	2002-07-04	David C. Reardon
6	20090256703	2009-10-15	Steve Bolton
7	20050269406	2005-12-08	Andrew C. Neff

If you wish to add additional U.S. Published Application citation information please click the Add button.

Add

FOREIGN PATENT DOCUMENTS

Remove

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	2012175758	WO		2012-12-27	Indra Sistemas, S.A.		

If you wish to add additional Foreign Patent Document citation information please click the Add button

Add

NON-PATENT LITERATURE DOCUMENTS

Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)

Application Number		16745621
Filing Date		2020-01-17
First Named Inventor	JAMES M. CANTER	
Art Unit		
Examiner Name		
Attorney Docket Number	HART:032C2	

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	Quesenbery, Making Voting Universal (And secure), Civic Designing, Medium.com, Printed From Internet January 2019, 9 pgs.	
	2	Unisyn Voting Solutions, OpenElect FreedomVote Tablet (FVT), The Freedom To Adapt, 2017, 2 pgs.	
	3	Election Systems & Software, ExpressVote XL, Full face Universal Voting System, 2016, 2 pgs.	
	4	Election Systems & Software, ExpressVote, Universal Voting System As A Marker, 2016, 2 pgs.	
	5	United States Patent Application No. 16/560,222 filed 9/4/2019, titled "Optical Character Recognition Of Voter Selections For Cast Vote Records," 22 pages.	

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/LAURA A GUDORE/	Date Considered	09/29/2020
--------------------	------------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16745621
Filing Date	2020-01-17
First Named Inventor	JAMES M. CANTER
Art Unit	
Examiner Name	
Attorney Docket Number	HART:032C2

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Richard D. Egan/	Date (YYYY-MM-DD)	2020-01-28
Name/Print	Richard D. Egan	Registration Number	36788

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Doc code: IDS

PTO/SB/08a (03-15)

Doc description: Information Disclosure Statement (IDS) Filed

Approved for use through 07/31/2016. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)

Application Number	16745621
Filing Date	2020-01-17
First Named Inventor	JAMES M. CANTER
Art Unit	
Examiner Name	
Attorney Docket Number	HART:032C2

U.S.PATENTS

Remove

Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/L.A.G/	1	5748807		1998-05-05	Lopresti et al.	
/L.A.G/	2	5703972		1997-12-30	Lopresti et al.	
/L.A.G/	3	5625721		1997-04-29	Lopresti et al.	

If you wish to add additional U.S. Patent citation information please click the Add button.

Add

U.S.PATENT APPLICATION PUBLICATIONS

Remove

Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

Add

FOREIGN PATENT DOCUMENTS

Remove

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²ⁱ	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)

Application Number	16745621
Filing Date	2020-01-17
First Named Inventor	JAMES M. CANTER
Art Unit	
Examiner Name	
Attorney Docket Number	HART:032C2

If you wish to add additional Foreign Patent Document citation information please click the Add button

Add

NON-PATENT LITERATURE DOCUMENTS

Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1		

If you wish to add additional non-patent literature document citation information please click the Add button

Add

EXAMINER SIGNATURE

Examiner Signature	/LAURA A GUDORF/	Date Considered	09/29/2020
--------------------	------------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16745621
Filing Date	2020-01-17
First Named Inventor	JAMES M. CANTER
Art Unit	
Examiner Name	
Attorney Docket Number	HART:032C2

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Richard D. Egan/	Date (YYYY-MM-DD)	2020-09-21
Name/Print	Richard D. Egan	Registration Number	36788

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Doc code: IDS

PTO/SB/08a (03-15)

Doc description: Information Disclosure Statement (IDS) Filed

Approved for use through 07/31/2016. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16745621
Filing Date	2020-01-17
First Named Inventor	JAMES M. CANTER
Art Unit	
Examiner Name	
Attorney Docket Number	HART:032C2

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	7306148		2007-12-11	Morganstein	
	2	5377099		1994-12-27	Miyagawa	
	3	6885758		2005-04-26	Bayer	
	4	5726435		1998-03-10	Hara et al.	
	5	2612994		1949-10-20	Woodland et al.	
	6	10147259		2018-12-04	Dvorak	
	7	10002481		2018-06-19	Seibel et al.	
	8	9165417		2015-10-20	Valles Fontanals et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16745621
Filing Date	2020-01-17
First Named Inventor	JAMES M. CANTER
Art Unit	
Examiner Name	
Attorney Docket Number	HART:032C2

9	6873966		2005-03-29	Babbitt et al.
10	7729991		2010-06-01	Rodriguez et al.
11	RE40449		2008-08-05	Provitola et al.
12	6250548		2001-06-26	McClure et al.
13	5764799		1998-06-09	Hong et al.
14	9361531		2016-06-07	Stella
15	3609685		1971-09-28	Deutsch
16	9401059		2016-07-26	Backert et al.
17	6971574		2005-12-06	Herskowitz
18	7080779		2006-07-25	Cummings
19	7406201		2008-07-29	Heilper et al.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)

Application Number	16745621
Filing Date	2020-01-17
First Named Inventor	JAMES M. CANTER
Art Unit	
Examiner Name	
Attorney Docket Number	HART:032C2

If you wish to add additional U.S. Patent citation information please click the Add button.

Add

U.S.PATENT APPLICATION PUBLICATIONS

Remove

Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20190213820		2019-07-11	Sebes et al.	
	2	20090166417		2009-07-02	Dammann et al.	
	3	20060041468		2006-02-23	Reardon	
	4	20140012635		2014-01-09	Joyce et al.	
	5	20100114674		2010-05-06	Daza Fernandez et al.	
	6	20110202464		2011-08-18	Carbullido	
	7	20180102013		2018-04-12	Spanos et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button.

Add

FOREIGN PATENT DOCUMENTS

Remove

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵
-------------------	---------	--------------------------------------	---------------------------	------------------------	------------------	---	--	----------------

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)

Application Number	16745621
Filing Date	2020-01-17
First Named Inventor	JAMES M. CANTER
Art Unit	
Examiner Name	
Attorney Docket Number	HART:032C2

1	0120562A2	WO		2001-03-22	Adler et al.		
2	2004038632	WO		2004-05-06	Boldin		
3	1020130185582	BR		2014-09-02	Nadaf		

If you wish to add additional Foreign Patent Document citation information please click the Add button

Add

NON-PATENT LITERATURE DOCUMENTS

Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	Kim et al., "Improved Support For Machine-Assisted Ballot-Level Audits", Usenix Journal Of Election Technology And Systems (JETS), Vol. 1, No. 1, August 2013, 18 pgs.	
	2	Keller et al., "A PC-Based Open-Source Voting Machine With An Accessible Voter-Verifiable Paper Ballot", Usenix, 2005, 12 pgs.	
	3	Mohapatra et al., "Spell Checker For OCR", International Journal Of Computer Science And Information Technologies", Vol. 4, No. 1, 2013, 7 pgs.	
	4	Bunke, "A Fast Algorithm For Finding The Nearest Neighbor Of A Word In A Dictionary", IAM-93-025, November 1993, 16 pgs.	
	5	Hassan et al., "Language Independent Text Correction Using Finite State Automata", IBM Cairo Technology Development Center, 2008, 6 pgs.	
	6	Toledo, "Election Tally Sheets Processing System", IAPR Workshop, 2016, 5 pgs.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)

Application Number		16745621
Filing Date		2020-01-17
First Named Inventor	JAMES M. CANTER	
Art Unit		
Examiner Name		
Attorney Docket Number		HART:032C2

7	Ashford, "QR Codes And Academic Libraries: Reaching Mobile Users", Faculty Publications- George Fox University Libraries, 2010, 6 pgs.
8	Barrera, "Optical Encryption And QR Codes: Secure And Noise-Free Information Retrieval", Optics Express, 2013, 6 pgs.
9	Krawczyk et al., "HMAC: Keyed-Hashing For Message Authentication", Network Working Group, February 1997, 11 pgs.
10	Essex et al., "Hover: Trustworthy Elections With Hash-Only Verification", IEEE Computer And Reliability Societies, 2012, 7 pgs.
11	Preneel, "The First 30 Years Of Cryptographic Hash Functions And The NIST SHA-3 Competition", Katholieke Universiteit Leuven and IBBT, Dept. Electrical Engineering, 2010, 15 pgs.
12	Shamos, "Electronic Voting Glossary", Carnegie Mellon University, 2011, 8 pgs.

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/LAURA A GUDORF/	Date Considered	09/29/2020
--------------------	------------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	16745621
Filing Date	2020-01-17
First Named Inventor	JAMES M. CANTER
Art Unit	
Examiner Name	
Attorney Docket Number	HART:032C2

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Richard D. Egan/	Date (YYYY-MM-DD)	2020-03-17
Name/Print	Richard D. Egan	Registration Number	36788

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (03-15)

Approved for use through 07/31/2016. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)

Application Number	16745621
Filing Date	2020-01-17
First Named Inventor	JAMES M. CANTER
Art Unit	
Examiner Name	
Attorney Docket Number	HART:032C2

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

Add

U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

Add

FOREIGN PATENT DOCUMENTS							Remove	
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²ⁱ	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵
/L.A.G/	1	1020130185582A2	BR		2014-09-02	Ronaldo Nadaf		

If you wish to add additional Foreign Patent Document citation information please click the Add button

Add

NON-PATENT LITERATURE DOCUMENTS				Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)

Application Number		16745621
Filing Date		2020-01-17
First Named Inventor	JAMES M. CANTER	
Art Unit		
Examiner Name		
Attorney Docket Number	HART:032C2	

/L.A.G/	1	Petition For Post Grant Review Of U.S. Patent No. 10,445,966, Election Systems & Software, LLC. v. Hart InterCivic, Inc., 99 pgs.
/L.A.G/	2	Declaration of Carlos Cezar Cordeiro Pires, Election Systems & Software, LLC. v. Hart InterCivic, Inc., Patent No. 10,445,966, 100 pgs.
/L.A.G/	3	Declaration of Michael I. Shamos, Ph.D., J.D., Election Systems & Software, LLC. v. Hart InterCivic, Inc., Patent No. 10,445,966, 175 pgs.
/L.A.G/	4	Petitioner's Power of Attorney, Election Systems & Software, LLC. v. Hart InterCivic, Inc., Patent No. 10,445,966, 3 pgs.
/L.A.G/	5	File History for Patent No. 10,445,966, 172 pgs.

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/LAURA A GUDORE/	Date Considered	09/29/2020
--------------------	------------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	16745621		
Filing Date	2020-01-17		
First Named Inventor	JAMES M. CANTER		
Art Unit			
Examiner Name			
Attorney Docket Number	HART:032C2		

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Richard D. Egan/	Date (YYYY-MM-DD)	2020-03-20
Name/Print	Richard D. Egan	Registration Number	36788

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L2	2	"20140231513"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/09/29 15:05
S1	40	("10002481" "10147259" "10445966" "10573111" "20020084325" "20050269406" "20060041468" "20090166417" "20090256703" "20090289115" "20100114674" "20110202464" "20140012635" "20140231513" "20170344538" "20180102013" "20180350180" "20190213820" "2612994" "3609685" "5377099" "5497318" "5726435" "5764799" "6250548" "6873966" "6885758" "6971574" "7080779" "7306148" "7406201" "7635088" "7729991" "7988047" "8261986" "8991701" "9165417" "9361531" "9401059" "RE40449").PN.	US-PGPUB; USPAT	OR	OFF	2020/09/15 07:18
S2	4,766	G07C13/00.cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/09/18 08:44
S3	3,489	S2 and @ay<"2019"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/09/18 08:45
S4	435	S3 and (barcode ((bar qr matrix 2d) adj2 code))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/09/18 08:47
S5	507	vote\$1 and (barcode ((bar qr matrix 2d) adj2 code)) same compar\$3	US-PGPUB; USPAT; USOCR; FPRS;	OR	OFF	2020/09/18 10:26

			EPO; JPO; DERWENT; IBM_TDB			
S6	95	vote\$1 same (barcode ((bar qr matrix 2d) adj2 code)) same compar\$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/09/18 10:26
S7	3	"20140203087"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/09/21 06:46
S8	714	ocr same (barcode ((bar qr matrix 2d) adj2 code)) same (comparing compare\$1)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/09/21 06:59
S10	10,306	G06K7/10346.cpc. G06K9/00442.cpc. G06K17/0032.cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2020/09/22 07:30
S11	26	((optical adj2 character adj2 recognition) OCR) same (concatenat\$3 with string)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/09/27 18:01
S12	2	((optical adj2 character adj2 recognition) OCR) same (recursiv\$3) same compari\$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/09/28 08:38
S13	64	((optical adj2 character adj2 recognition) OCR) same (recursiv\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/09/28 08:39
S14	574	((optical adj2 character adj2 recognition) OCR) with repeat\$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO;	OR	ON	2020/09/28 08:43

			DERWENT; IBM_TDB			
S15	167	((optical adj2 character adj2 recognition) OCR) with mismatch	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/09/28 08:47
S16	156	((optical adj2 character adj2 recognition) OCR) same (compari\$3 with distance\$1)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/09/28 09:31

9/29/2020 3:38:57 PM

C:\Users\lgudorf\Documents\EAST\Workspaces\16919267.wsp

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (03-15)

Approved for use through 07/31/2016. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)

Application Number	16745621
Filing Date	2020-01-17
First Named Inventor	JAMES M. CANTER
Art Unit	
Examiner Name	
Attorney Docket Number	HART:032C2

U.S.PATENTS							Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	
	1						
If you wish to add additional U.S. Patent citation information please click the Add button.							Add
U.S.PATENT APPLICATION PUBLICATIONS							Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	
	1						
If you wish to add additional U.S. Published Application citation information please click the Add button.							Add
FOREIGN PATENT DOCUMENTS							Remove
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²ⁱ	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1						
If you wish to add additional Foreign Patent Document citation information please click the Add button							Add
NON-PATENT LITERATURE DOCUMENTS							Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.					T ⁵

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16745621	
Filing Date	2020-01-17	
First Named Inventor	JAMES M. CANTER	
Art Unit		
Examiner Name		
Attorney Docket Number	HART:032C2	

/L.A.G./ ¹	Election Systems & Software, LLC. v. Hart InterCivic, Inc., Patent No. 10,445,966, Decision Granting Institution Of Post-Grant Review 35 U.S.C. § 324, 37 C.F.R. § 42.4, September 2, 2020, 48 pgs.
-----------------------	---

If you wish to add additional non-patent literature document citation information please click the Add button

Add

EXAMINER SIGNATURE

Examiner Signature	/LAURA A GUDORE/	Date Considered	09/29/2020
--------------------	------------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16745621		
Filing Date	2020-01-17		
First Named Inventor	JAMES M. CANTER		
Art Unit			
Examiner Name			
Attorney Docket Number	HART:032C2		

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Richard D. Egan/	Date (YYYY-MM-DD)	2020-09-14
Name/Print	Richard D. Egan	Registration Number	36788

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Bibliographic Data

Application No: 16/745,621

Foreign Priority claimed: ☐ Yes ☒ No

35 USC 119 (a-d) conditions met: ☐ Yes ☒ No ☐ Met After Allowance

Verified and Acknowledged: /LAURA A GUDORF/

Examiner's Signature

Initials

Title:

Optical Character Recognition Of Voter Selections For Cast Vote Records

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
01/17/2020	235	2876	HART:032C2
RULE			

APPLICANTS

Hart InterCivic, Inc., Austin, TX, UNITED STATES

INVENTORS

James M. Canter, Austin, TX, UNITED STATES

Drew E. Tinney, Austin, TX, UNITED STATES

Ievgen Konovalenko, Austin, TX, UNITED STATES

CONTINUING DATA

This application is a CON of 16560222 09/04/2019 PAT 10573111

16560222 is a CON of 16239607 01/04/2019 PAT 10445966

16239607 has PRO of 62711212 07/27/2018

FOREIGN APPLICATIONS

IF REQUIRED, FOREIGN LICENSE GRANTED**

02/04/2020

STATE OR COUNTRY

UNITED STATES

ADDRESS

Egan, Peterman, Enders & Huston LLP.

1101 S. Capital of Texas Highway

Bldg C, Suite 200

Austin, TX 78746

UNITED STATES

FILING FEE RECEIVED

\$1,920

Electronic Acknowledgement Receipt

EFS ID:	40631617
Application Number:	16745621
International Application Number:	
Confirmation Number:	6960
Title of Invention:	Optical Character Recognition Of Voter Selections For Cast Vote Records
First Named Inventor/Applicant Name:	James M. Canter
Customer Number:	36275
Filer:	Richard D. Egan/Marty Jones
Filer Authorized By:	Richard D. Egan
Attorney Docket Number:	HART:032C2
Receipt Date:	22-SEP-2020
Filing Date:	17-JAN-2020
Time Stamp:	16:01:51
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Preliminary Amendment	3rdPreliminaryAmendment.pdf	34928 1e204ba49cd3b2e52b37b9b224b904d4137c61cc	no	6

Warnings:

Information:	
Total Files Size (in bytes):	34928
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>	

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: JAMES M. CANTER ET AL.

Filed: JANUARY 17, 2020

For: OPTICAL CHARACTER RECOGNITION OF VOTER SELECTIONS
FOR CAST VOTE RECORDS

Serial No.: 16/745,621

Group Art Unit: UNKNOWN

Examiner: UNKNOWN

Atty Docket No.: HART:032C2

Electronically filed with the PTO

Commissioner For Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

THIRD PRELIMINARY AMENDMENT

Please amend the application as follows.

Amendments to the Claims

Please amend Claims 1 and 18 as follows:

1. (Currently Amended) A method for electronic voting using printed vote records, comprising:

generating a printed vote record of at least one vote selection of a voter;

providing, on the printed vote record, voter readable text indicating the voter's at least one vote selection;

providing, on the printed vote record, encoded data, the encoded data ~~indicating~~ based at least in part on the voter's at least one vote selection;

electronically scanning the voter readable text on the printed vote record to create a first data set, the first data set ~~indicating at least~~ based at least in part on the voter's at least one vote selection;

electronically scanning the encoded data on the printed vote record to create a second data set, the second data set ~~indicating at least~~ based at least in part on the voter's at least one vote selection;

comparing the first data set and the second data set; and

providing a cast vote record indicating the voter's at least one vote selection, an accuracy of the cast vote record confirmed based at least in part on a comparison of ~~the voter's at least one vote selection as indicated by the~~ first data set and ~~the voter's at least one vote selection as indicated by the~~ second data set.

2. (Original) The method of claim 1, wherein the encoded data includes at least one bar code.

3. (Original) The method of claim 2, wherein the bar code is a one dimensional bar code.
4. (Original) The method of claim 1, wherein the bar code is a two dimensional bar code.
5. (Original) The method of claim 4, wherein the two dimensional bar code is a QR code bar code.
6. (Previously Presented) The method of claim 1, further comprising confirming an integrity of the printed vote record based at least in part on a comparison of the first data set and the second data set.
7. (Previously Presented) The method of claim 6, wherein confirming the integrity of the printed vote record comprises comparing the first data set to information provided in the encoded data.
8. (Previously Presented) The method of claim 7, wherein confirming the integrity of the printed vote record comprises comparing a first hash produced from the first data set to a second hash provided in the encoded data.
9. (Original) The method of claim 6, further comprising comparing the first data set to an election dictionary, the election dictionary containing at least potential vote choices.

10. (Original) The method of claim 9, wherein the comparing the first data set to an election dictionary is utilized to confirm the accuracy of an optical character recognition (OCR) process.

11. (Original) The method of claim 1, further comprising comparing the first data set to an election dictionary, the election dictionary containing at least potential vote choices.

12. (Previously Presented) The method of claim 11, wherein the comparing the first data set to an election dictionary is utilized to confirm the accuracy of an optical character recognition (OCR) process.

13. (Original) The method of claim 12, wherein the election dictionary contains at least one candidate name.

14. (Original) The method of claim 1, wherein the encoded data includes at least one bar code, bar code data of the bar code including data which is used to map the bar code to at least one particular vote selection.

15. (Previously Presented) The method of claim 14, wherein the at least one particular vote selection is a particular candidate.

16. (Previously Presented) The method of claim 14, wherein the data which is used to map the bar code to at least one particular vote selection is hash data.

17. (Previously Presented) The method of claim 14, wherein the bar code data of the bar code maps to the at least one particular vote selection through the use of a hash.

18. (Currently Amended) The method of claim 1, wherein the comparison of the first data set and the second data set is used to confirm that the at least one vote selection that the first data set is based at least in part on ~~indicated by the first data set~~ matches the at least one vote selection that the second data set is based at least in part on ~~indicated by the second data set~~.

19. (Original) The method of claim 1, further comprising utilizing an election dictionary as part of the process to provide a cast vote record.

20. (Original) The method of claim 19, wherein the election dictionary includes at least a candidate name and other data affiliated with candidate name.

21. (Original) The method of claim 20, wherein the other data affiliated with a candidate name is a number.

22. (Original) The method of claim 21, wherein the number is a candidate sequence number or number indicative of a line of the printed vote record.

REMARKS

Should any fees under 37 CFR 1.16-1.21 be required for any reason relating to the enclosed materials, the Commissioner is authorized to deduct such fees from Deposit Account No. 10-1205/HART:032C2. The examiner is invited to contact the undersigned at the phone number indicated below with any questions or comments, or to otherwise facilitate expeditious and compact prosecution of the application.

Respectfully submitted,

/Richard D. Egan/
Richard D. Egan
Registration No.: 36,788
Attorney for Applicant

EGAN, PETERMAN, ENDERS & HUSTON, LLP
1101 South Capital of Texas Highway
Building C, Suite 200
Austin, Texas 78746
(512) 347-1611
FAX: (512) 347-1615

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875				Application or Docket Number 16/745,621		Filing Date 01/17/2020		☐ To be Mailed				
ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO												
APPLICATION AS FILED - PART I												
		(Column 1)	(Column 2)									
FOR		NUMBER FILED	NUMBER EXTRA		RATE (\$)		FEE (\$)					
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))		N/A	N/A		N/A							
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))		N/A	N/A		N/A							
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))		N/A	N/A		N/A							
TOTAL CLAIMS (37 CFR 1.16(i))		minus 20 = *				x \$100 =						
INDEPENDENT CLAIMS (37 CFR 1.16(h))		minus 3 = *				x \$460 =						
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))		If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).										
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))												
* If the difference in column 1 is less than zero, enter "0" in column 2.						TOTAL						
APPLICATION AS AMENDED - PART II												
		(Column 1)	(Column 2)		(Column 3)							
AMENDMENT	09/22/2020	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)		ADDITIONAL FEE (\$)				
	Total (37 CFR 1.16(i))	* 22	Minus	** 22	= 0	x \$100 =		0				
	Independent (37 CFR 1.16(h))	* 1	Minus	*** 3	= 0	x \$460 =		0				
	☐ Application Size Fee (37 CFR 1.16(s))											
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))											
								TOTAL ADD'L FEE		0		
		(Column 1)	(Column 2)		(Column 3)							
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)		ADDITIONAL FEE (\$)				
	Total (37 CFR 1.16(i))	*	Minus	**	=	x \$0 =						
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x \$0 =						
	☐ Application Size Fee (37 CFR 1.16(s))											
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))											
								TOTAL ADD'L FEE				
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.						SLIE						
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".						/SHARON M WEST/						
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".												
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.												

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		16745621
	Filing Date		2020-01-17
	First Named Inventor	JAMES M. CANTER	
	Art Unit		
	Examiner Name		
	Attorney Docket Number		HART:032C2

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5748807		1998-05-05	Lopresti et al.	
	2	5703972		1997-12-30	Lopresti et al.	
	3	5625721		1997-04-29	Lopresti et al.	

If you wish to add additional U.S. Patent citation information please click the Add button.

Add

U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

Add

FOREIGN PATENT DOCUMENTS								Remove
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² i	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		16745621
	Filing Date		2020-01-17
	First Named Inventor	JAMES M. CANTER	
	Art Unit		
	Examiner Name		
	Attorney Docket Number	HART:032C2	

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS			<input type="button" value="Remove"/>
--	--	--	---------------------------------------

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1		

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16745621
Filing Date	2020-01-17
First Named Inventor	JAMES M. CANTER
Art Unit	
Examiner Name	
Attorney Docket Number	HART:032C2

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Richard D. Egan/	Date (YYYY-MM-DD)	2020-09-21
Name/Print	Richard D. Egan	Registration Number	36788

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	40610882
Application Number:	16745621
International Application Number:	
Confirmation Number:	6960
Title of Invention:	Optical Character Recognition Of Voter Selections For Cast Vote Records
First Named Inventor/Applicant Name:	James M. Canter
Customer Number:	36275
Filer:	Richard D. Egan/Marty Jones
Filer Authorized By:	Richard D. Egan
Attorney Docket Number:	HART:032C2
Receipt Date:	21-SEP-2020
Filing Date:	17-JAN-2020
Time Stamp:	11:14:21
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	IDS_5.pdf	1034964	no	4
			e66227a96459d6c3bcff39ee94471dea4aee754b		

Warnings:

Information:	
Total Files Size (in bytes):	1034964
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	16745621
	Filing Date	2020-01-17
	First Named Inventor	JAMES M. CANTER
	Art Unit	
	Examiner Name	
	Attorney Docket Number	HART:032C2

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

Add

U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

Add

FOREIGN PATENT DOCUMENTS							Remove	
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²ⁱ	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button

Add

NON-PATENT LITERATURE DOCUMENTS			Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		16745621
	Filing Date		2020-01-17
	First Named Inventor	JAMES M. CANTER	
	Art Unit		
	Examiner Name		
	Attorney Docket Number	HART:032C2	

1	Election Systems & Software, LLC. v. Hart InterCivic, Inc., Patent No. 10,445,966, Decision Granting Institution Of Post-Grant Review 35 U.S.C. § 324, 37 C.F.R. § 42.4, September 2, 2020, 48 pgs.
---	---

If you wish to add additional non-patent literature document citation information please click the Add button

Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16745621
Filing Date	2020-01-17
First Named Inventor	JAMES M. CANTER
Art Unit	
Examiner Name	
Attorney Docket Number	HART:032C2

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Richard D. Egan/	Date (YYYY-MM-DD)	2020-09-14
Name/Print	Richard D. Egan	Registration Number	36788

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	40550807
Application Number:	16745621
International Application Number:	
Confirmation Number:	6960
Title of Invention:	Optical Character Recognition Of Voter Selections For Cast Vote Records
First Named Inventor/Applicant Name:	James M. Canter
Customer Number:	36275
Filer:	Richard D. Egan/Marty Jones
Filer Authorized By:	Richard D. Egan
Attorney Docket Number:	HART:032C2
Receipt Date:	14-SEP-2020
Filing Date:	17-JAN-2020
Time Stamp:	16:23:32
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	IDS_3.pdf	1035050	no	4
			5aaf25c2b44fbce6c8d98f4584753789bd540560		

Warnings:

Information:					
A U.S. Patent Number Citation or a U.S. Publication Number Citation is required in the Information Disclosure Statement (IDS) form for autoloading of data into USPTO systems. You may remove the form to add the required data in order to correct the Informational Message if you are citing U.S. References. If you chose not to include U.S. References, the image of the form will be processed and be made available within the Image File Wrapper (IFW) system. However, no data will be extracted from this form. Any additional data such as Foreign Patent Documents or Non Patent Literature will be manually reviewed and keyed into USPTO systems.					
2	Non Patent Literature	C1.pdf	817447	no	48
			1ab3ef80061b606dcae4834a76a1c3b0dc5137e2		
Warnings:					
Information:					
Total Files Size (in bytes):				1852497	
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875				Application or Docket Number 16/745,621		Filing Date 01/17/2020		☐ To be Mailed		
ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO										
APPLICATION AS FILED - PART I										
		(Column 1)	(Column 2)							
FOR		NUMBER FILED	NUMBER EXTRA	RATE (\$)		FEE (\$)				
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))		N/A	N/A	N/A						
☐ SEARCH FEE (37 CFR 1.16(k), (l), or (m))		N/A	N/A	N/A						
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))		N/A	N/A	N/A						
TOTAL CLAIMS (37 CFR 1.16(i))		minus 20 =	*	x \$100 =						
INDEPENDENT CLAIMS (37 CFR 1.16(h))		minus 3 =	*	x \$460 =						
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))		If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).								
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))										
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL						
APPLICATION AS AMENDED - PART II										
		(Column 1)	(Column 2)	(Column 3)						
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)		ADDITIONAL FEE (\$)		
	Total (37 CFR 1.16(i))	*	Minus	**	=	x \$0 =				
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x \$0 =				
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
						TOTAL ADD'L FEE				
		(Column 1)	(Column 2)	(Column 3)						
AMENDMENT	06/30/2020	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)		ADDITIONAL FEE (\$)		
	Total (37 CFR 1.16(i))	* 22	Minus	** 22	= 0	x \$100 =		0		
	Independent (37 CFR 1.16(h))	* 1	Minus	*** 3	= 0	x \$460 =		0		
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
						TOTAL ADD'L FEE		0		
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.						LDRC				
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".						/EVA V GILLIS/				
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".										
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.										

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Acknowledgement Receipt

EFS ID:	39868750
Application Number:	16745621
International Application Number:	
Confirmation Number:	6960
Title of Invention:	Optical Character Recognition Of Voter Selections For Cast Vote Records
First Named Inventor/Applicant Name:	James M. Canter
Customer Number:	36275
Filer:	Richard D. Egan/Marty Jones
Filer Authorized By:	Richard D. Egan
Attorney Docket Number:	HART:032C2
Receipt Date:	30-JUN-2020
Filing Date:	17-JAN-2020
Time Stamp:	12:54:31
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Preliminary Amendment	2ndPreliminaryAmendment. pdf	34355	no	6
			42b608594ddc9dbed1dd4304d1bfa3c6ea 0e80bf		

Warnings:

Information:	
Total Files Size (in bytes):	34355
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>	

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: JAMES M. CANTER ET AL.

Filed: JANUARY 17, 2020

For: OPTICAL CHARACTER RECOGNITION OF VOTER SELECTIONS
FOR CAST VOTE RECORDS

Serial No.: 16/745,621

Group Art Unit: UNKNOWN

Examiner: UNKNOWN

Atty Docket No.: HART:032C2

Electronically filed with the PTO

Commissioner For Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

SECOND PRELIMINARY AMENDMENT

Please amend the application as follows.

Amendments to the Claims

Please amend Claim 17 as follows:

1. (Previously Presented) A method for electronic voting using printed vote records, comprising:

generating a printed vote record of at least one vote selection of a voter;

providing, on the printed vote record, voter readable text indicating the voter's at least one vote selection;

providing, on the printed vote record, encoded data, the encoded data indicating the voter's at least one vote selection;

electronically scanning the voter readable text on the printed vote record to create a first data set, the first data set indicating at least the voter's at least one vote selection;

electronically scanning the encoded data on the printed vote record to create a second data set, the second data set indicating at least the voter's at least one vote selection;

comparing the first data set and the second data set; and

providing a cast vote record indicating the voter's at least one vote selection, an accuracy of the cast vote record confirmed based at least in part on a comparison of the voter's at least one vote selection as indicated by the first data set and the voter's at least one vote selection as indicated by the second data set.

2. (Original) The method of claim 1, wherein the encoded data includes at least one bar code.

3. (Original) The method of claim 2, wherein the bar code is a one dimensional bar code.
4. (Original) The method of claim 1, wherein the bar code is a two dimensional bar code.
5. (Original) The method of claim 4, wherein the two dimensional bar code is a QR code bar code.
6. (Previously Presented) The method of claim 1, further comprising confirming an integrity of the printed vote record based at least in part on a comparison of the first data set and the second data set.
7. (Previously Presented) The method of claim 6, wherein confirming the integrity of the printed vote record comprises comparing the first data set to information provided in the encoded data.
8. (Previously Presented) The method of claim 7, wherein confirming the integrity of the printed vote record comprises comparing a first hash produced from the first data set to a second hash provided in the encoded data.
9. (Original) The method of claim 6, further comprising comparing the first data set to an election dictionary, the election dictionary containing at least potential vote choices.

10. (Original) The method of claim 9, wherein the comparing the first data set to an election dictionary is utilized to confirm the accuracy of an optical character recognition (OCR) process.

11. (Original) The method of claim 1, further comprising comparing the first data set to an election dictionary, the election dictionary containing at least potential vote choices.

12. (Previously Presented) The method of claim 11, wherein the comparing the first data set to an election dictionary is utilized to confirm the accuracy of an optical character recognition (OCR) process.

13. (Original) The method of claim 12, wherein the election dictionary contains at least one candidate name.

14. (Original) The method of claim 1, wherein the encoded data includes at least one bar code, bar code data of the bar code including data which is used to map the bar code to at least one particular vote selection.

15. (Previously Presented) The method of claim 14, wherein the at least one particular vote selection is a particular candidate.

16. (Previously Presented) The method of claim 14, wherein the data which is used to map the bar code to at least one particular vote selection is hash data.

17. (Currently Amended) The method of claim 14, wherein the bar code data of the bar code maps to the at least one particular vote selection through the use of a hash.

18. (Original) The method of claim 1, wherein the comparison of the first data set and the second data set is used to confirm that the at least one vote selection indicated by the first data set matches the at least one vote selection indicated by the second data set.

19. (Original) The method of claim 1, further comprising utilizing an election dictionary as part of the process to provide a cast vote record.

20. (Original) The method of claim 19, wherein the election dictionary includes at least a candidate name and other data affiliated with candidate name.

21. (Original) The method of claim 20, wherein the other data affiliated with a candidate name is a number.

22. (Original) The method of claim 21, wherein the number is a candidate sequence number or number indicative of a line of the printed vote record.

REMARKS

Should any fees under 37 CFR 1.16-1.21 be required for any reason relating to the enclosed materials, the Commissioner is authorized to deduct such fees from Deposit Account No. 10-1205/HART:032C2. The examiner is invited to contact the undersigned at the phone number indicated below with any questions or comments, or to otherwise facilitate expeditious and compact prosecution of the application.

Respectfully submitted,

/Richard D. Egan/
Richard D. Egan
Registration No.: 36,788
Attorney for Applicant

EGAN, PETERMAN, ENDERS & HUSTON, LLP
1101 South Capital of Texas Highway
Building C, Suite 200
Austin, Texas 78746
(512) 347-1611
FAX: (512) 347-1615

Electronic Acknowledgement Receipt

EFS ID:	39858174
Application Number:	16745621
International Application Number:	
Confirmation Number:	6960
Title of Invention:	Optical Character Recognition Of Voter Selections For Cast Vote Records
First Named Inventor/Applicant Name:	James M. Canter
Customer Number:	36275
Filer:	Richard D. Egan/Marty Jones
Filer Authorized By:	Richard D. Egan
Attorney Docket Number:	HART:032C2
Receipt Date:	29-JUN-2020
Filing Date:	17-JAN-2020
Time Stamp:	16:14:26
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Preliminary Amendment	PreliminaryAmendment.pdf	34759	no	6
			85c0b751d214bf38c7a65137a2e2c65e5ba bea7b		

Warnings:

Information:	
Total Files Size (in bytes):	34759
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>	

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: JAMES M. CANTER ET AL.

Filed: JANUARY 17, 2020

For: OPTICAL CHARACTER RECOGNITION OF VOTER SELECTIONS
FOR CAST VOTE RECORDS

Serial No.: 16/745,621

Group Art Unit: UNKNOWN

Examiner: UNKNOWN

Atty Docket No.: HART:032C2

Electronically filed with the PTO

Commissioner For Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

PRELIMINARY AMENDMENT

Please amend the application as follows.

Amendments to the Claims

Please amend Claims 1, 6-8, 12 and 15-16 as follows:

1. (Currently Amended) A method for electronic voting using printed vote records, comprising:

generating a printed vote record of at least one vote selection of a voter;

providing, on the printed vote record, voter readable text indicating the voter's at least one vote selection;

providing, on the printed vote record, encoded data, the encoded data indicating the voter's at least one vote selection;

electronically scanning the voter readable text on the printed vote record to create a first data set, the first data set indicating at least the voter's at least one vote selection;

electronically scanning the encoded data on the printed vote record to create a second data set, the second data set indicating at least the voter's at least one vote selection;

comparing the first data set and the second data set; and

providing a cast vote record indicating the voter's at least one vote selection, an accuracy of the cast vote record confirmed based at least in part on a comparison of the voter's at least one vote selection as indicated by the first data set and the voter's at least one vote selection as indicated by the second data set.

2. (Original) The method of claim 1, wherein the encoded data includes at least one bar code.

3. (Original) The method of claim 2, wherein the bar code is a one dimensional bar code.
4. (Original) The method of claim 1, wherein the bar code is a two dimensional bar code.
5. (Original) The method of claim 4, wherein the two dimensional bar code is a QR code bar code.
6. (Currently Amended) The method of claim 1, further comprising confirming an integrity of the printed vote record based at least in part on a comparison of the first data set and the second data set. ~~utilizing the first data set and the second data set to confirm an integrity of the printed vote record.~~
7. (Currently Amended) The method of claim 6, wherein confirming the integrity of the printed vote record ~~is confirmed by~~ comprises comparing the first data set to information provided in the encoded data.
8. (Currently Amended) The method of claim 7, wherein confirming the integrity of the printed vote record ~~is confirmed by~~ comprises comparing a first hash produced from the first data set to a second hash provided in the encoded data.

9. (Original) The method of claim 6, further comprising comparing the first data set to an election dictionary, the election dictionary containing at least potential vote choices.

10. (Original) The method of claim 9, wherein the comparing the first data set to an election dictionary is utilized to confirm the accuracy of an optical character recognition (OCR) process.

11. (Original) The method of claim 1, further comprising comparing the first data set to an election dictionary, the election dictionary containing at least potential vote choices.

12. (Currently Amended) The method of claim 11, wherein the comparing the first data set to an election dictionary is utilized to confirm the accuracy of ~~to confirm the accuracy~~ of an optical character recognition (OCR) process.

13. (Original) The method of claim 12, wherein the election dictionary contains at least one candidate name.

14. (Original) The method of claim 1, wherein the encoded data includes at least one bar code, bar code data of the bar code including data which is used to map the bar code to at least one particular vote selection.

15. (Currently Amended) The method of claim 14, wherein the at least one particular vote selection ~~choice~~ is a particular candidate.

16. (Currently Amended) The method of claim 14, wherein the data which is used to map the bar code to at least one particular vote selection ~~choice~~ is hash data.

17. (Original) The method of claim 14, wherein the bar code data of bar code maps to the at least one particular vote selection through the use of a hash.

18. (Original) The method of claim 1, wherein the comparison of the first data set and the second data set is used to confirm that the at least one vote selection indicated by the first data set matches the at least one vote selection indicated by the second data set.

19. (Original) The method of claim 1, further comprising utilizing an election dictionary as part of the process to provide a cast vote record.

20. (Original) The method of claim 19, wherein the election dictionary includes at least a candidate name and other data affiliated with candidate name.

21. (Original) The method of claim 20, wherein the other data affiliated with a candidate name is a number.

22. (Original) The method of claim 21, wherein the number is a candidate sequence number or number indicative of a line of the printed vote record.

REMARKS

Should any fees under 37 CFR 1.16-1.21 be required for any reason relating to the enclosed materials, the Commissioner is authorized to deduct such fees from Deposit Account No. 10-1205/HART:032C2. The examiner is invited to contact the undersigned at the phone number indicated below with any questions or comments, or to otherwise facilitate expeditious and compact prosecution of the application.

Respectfully submitted,

/Richard D. Egan/
Richard D. Egan
Registration No.: 36,788
Attorney for Applicant

EGAN, PETERMAN, ENDERS & HUSTON, LLP
1101 South Capital of Texas Highway
Building C, Suite 200
Austin, Texas 78746
(512) 347-1611
FAX: (512) 347-1615

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875				Application or Docket Number 16/745,621		Filing Date 01/17/2020		☐ To be Mailed		
ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO										
APPLICATION AS FILED - PART I										
		(Column 1)	(Column 2)							
FOR		NUMBER FILED	NUMBER EXTRA	RATE (\$)		FEE (\$)				
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))		N/A	N/A	N/A						
☐ SEARCH FEE (37 CFR 1.16(k), (l), or (m))		N/A	N/A	N/A						
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))		N/A	N/A	N/A						
TOTAL CLAIMS (37 CFR 1.16(i))		minus 20 =	*	x \$100 =						
INDEPENDENT CLAIMS (37 CFR 1.16(h))		minus 3 =	*	x \$460 =						
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))		If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).								
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))										
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL						
APPLICATION AS AMENDED - PART II										
		(Column 1)	(Column 2)	(Column 3)						
AMENDMENT	06/29/2020	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)		ADDITIONAL FEE (\$)		
	Total (37 CFR 1.16(i))	* 22	Minus	** 22	= 0	x \$100 =		0		
	Independent (37 CFR 1.16(h))	* 1	Minus	*** 3	= 0	x \$460 =		0		
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
						TOTAL ADD'L FEE		0		
		(Column 1)	(Column 2)	(Column 3)						
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)		ADDITIONAL FEE (\$)		
	Total (37 CFR 1.16(i))	*	Minus	**	=	x \$0 =				
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x \$0 =				
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
						TOTAL ADD'L FEE				
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.						LDRC				
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".						/EVA V GILLIS/				
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".										
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.										

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
16/745,621	01/17/2020	James M. Canter	HART:032C2

CONFIRMATION NO. 6960

PUBLICATION NOTICE



OC000000117084447

36275
Egan, Peterman, Enders & Huston LLP.
1101 S. Capital of Texas Highway
Bldg C, Suite 200
Austin, TX 78746

Title:Optical Character Recognition Of Voter Selections For Cast Vote Records

Publication No.US-2020-0151990-A1

Publication Date:05/14/2020

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently <http://www.uspto.gov/patft/>.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Public Records Division. The Public Records Division can be reached by telephone at (571) 272-3150 or (800) 972-6382, by facsimile at (571) 273-3250, by mail addressed to the United States Patent and Trademark Office, Public Records Division, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently <https://portal.uspto.gov/pair/PublicPair>. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		16745621
	Filing Date		2020-01-17
	First Named Inventor	JAMES M. CANTER	
	Art Unit		
	Examiner Name		
	Attorney Docket Number		HART:032C2

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

Add

U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

Add

FOREIGN PATENT DOCUMENTS							Remove	
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²ⁱ	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	1020130185582A2	BR		2014-09-02	Ronaldo Nadaf		

If you wish to add additional Foreign Patent Document citation information please click the Add button

Add

NON-PATENT LITERATURE DOCUMENTS			Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number		16745621
Filing Date		2020-01-17
First Named Inventor	JAMES M. CANTER	
Art Unit		
Examiner Name		
Attorney Docket Number	HART:032C2	

1	Petition For Post Grant Review Of U.S. Patent No. 10,445,966, Election Systems & Software, LLC. v. Hart InterCivic, Inc., 99 pgs.
2	Declaration of Carlos Cezar Cordeiro Pires, Election Systems & Software, LLC. v. Hart InterCivic, Inc., Patent No. 10,445,966, 100 pgs.
3	Declaration of Michael I. Shamos, Ph.D., J.D., Election Systems & Software, LLC. v. Hart InterCivic, Inc., Patent No. 10,445,966, 175 pgs.
4	Petitioner's Power of Attorney, Election Systems & Software, LLC. v. Hart InterCivic, Inc., Patent No. 10,445,966, 3 pgs.
5	File History for Patent No. 10,445,966, 172 pgs.

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16745621
Filing Date	2020-01-17
First Named Inventor	JAMES M. CANTER
Art Unit	
Examiner Name	
Attorney Docket Number	HART:032C2

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Richard D. Egan/	Date (YYYY-MM-DD)	2020-03-20
Name/Print	Richard D. Egan	Registration Number	36788

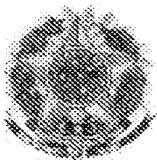
This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.



República Federativa do Brasil
Ministério do Desenvolvimento, Indústria
e Comércio Exterior
Instituto Nacional da Propriedade Industrial

(21) BR 10 2013 018558-2 A2

(22) Data de Depósito: 19/07/2013

(43) Data da Publicação: 02/09/2014
(RPI 2278)



* B R 1 0 2 0 1 3 0 1 8 5 5 8 A 2 *

(51) Int.Cl.:

G07C 13/00

G06K 9/46

G06Q 50/00

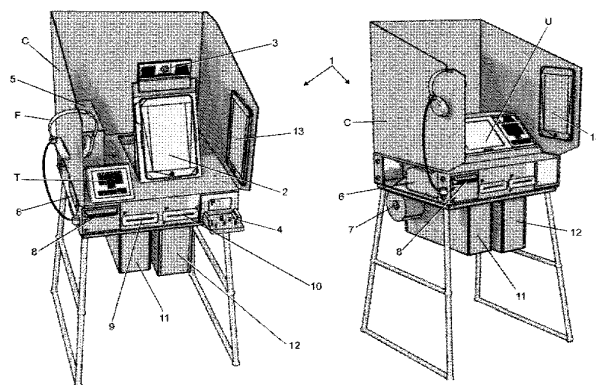
(54) **Título:** EQUIPAMENTO DE IMPRESSÃO E COLETA DE CÉDULAS DE SEGURANÇA DO VOTO E EQUIPAMENTO DE AUDITORIA E APURAÇÃO DE VOTOS IMPRESSOS EM CÉDULAS DE SEGURANÇA, PARA MODELO DE VOTAÇÃO MECATRÔNICA

(73) **Titular(es):** Ronaldo Moises Nadaf

(72) **Inventor(es):** Ronaldo Moises Nadaf

(74) **Procurador(es):** MODAL MARCAS E PATENTES LTDA

(57) **Resumo:** EQUIPAMENTO DE IMPRESSÃO E COLETA DE CÉDULAS DE SEGURANÇA DO VOTO E EQUIPAMENTO DE AUDITORIA E APURAÇÃO DE VOTOS IMPRESSOS EM CÉDULAS DE SEGURANÇA, PARA MODELO DE VOTAÇÃO MECATRÔNICA", onde um equipamento (1) forma um sistema que possibilita ao próprio eleitor, votar e obter uma cédula de impressão (14) pela qual serão confirmados, o voto eletrônico e a impressão, através de códigos de barra (15), (16), (17) e (18) nela gravados. Tal cédula (13) é transferida para um segundo equipamento (19), de apuração de votos, onde tais informações serão lidas, formando um sistema de armazenamento eletrônico e impresso, em total interação e passível de ser auditado, caso hajam dúvidas em relação a fraudes, trazendo total segurança ao sistema eleitoral.



“EQUIPAMENTO DE IMPRESSÃO E COLETA DE CÉDULAS DE
SEGURANÇA DO VOTO E EQUIPAMENTO DE AUDITORIA E
APURAÇÃO DE VOTOS IMPRESSOS EM CÉDULAS DE
SEGURANÇA, PARA MODELO DE VOTAÇÃO MECATRÔNICA”

5 Refere-se o presente pedido de patente de invenção para um conjunto de equipamentos que irão garantir a qualquer cidadão a votação eletrônica combinada à possibilidade de conferir o registro fiel de sua intenção política, utilizando cédulas de votação em papel como mecanismo de auditoria e segurança do voto individual.

10 Este conjunto de equipamentos vai trazer o voto impresso em cédulas de papel ao processo eleitoral, porém, com outro nível de segurança, onde a cédula impressa com o voto do cidadão será manuseada tão somente pelo eleitor votante.

15 O primeiro equipamento, denominado EQUIPAMENTO DE IMPRESSÃO E COLETA DE CÉDULAS DE SEGURANÇA DO VOTO, vai permitir, além da impressão do voto, ampliar a segurança da identificação do eleitor, pois tem como objetivo a utilização de um processo com o duplo reconhecimento biométrico do eleitor, onde serão verificadas, além das impressões digitais de 4 dedos da mão, um
20 reconhecimento biométrico da face.

A cédula de votação produzida nesse novo contexto tecnológico trará a impressão de no mínimo 2 registros do voto individual, sendo o primeiro registro em texto, produzido pelos sistemas digitais do

equipamento de voto digital, incluindo as urnas eletrônicas hoje em uso, e um segundo registro do voto, que será gerado pelo EQUIPAMENTO DE IMPRESSÃO E COLETA DE CÉDULAS DE SEGURANÇA DO VOTO, objeto desta patente, dito voto impresso, na mesma cédula, em códigos de barras bidimensional, ampliando ainda mais a segurança, a transparência e os mecanismos de auditoria do processo de geração e coleta dos votos.

Além dos dois registros do voto individual, um em texto e outro em código de barras, a cédula impressa trará mais dois registros em código de barras bidimensional que armazenarão as assinaturas digitais da Justiça Eleitoral e de outra instituição responsável pela auditoria do processo.

Essas assinaturas digitais serão produzidas por criptografia assimétrica de algoritmo ECDSA(Elliptic Curve Digital Signature Algorithm), com par de chaves de tamanho mínimo de 283 bit. O processo de assinatura do voto se dará pelas chaves privadas das instituições, que estarão instaladas no EQUIPAMENTO DE IMPRESSÃO E COLETA DE CÉDULAS DE SEGURANÇA DO VOTO e no computador coletor de votos, garantindo procedência institucional ao voto impresso, sem violar o sigilo do mesmo.

Um segundo equipamento presente neste pedido de patente de invenção, denominado EQUIPAMENTO DE AUDITORIA E APURAÇÃO DE VOTOS IMPRESSOS EM CÉDULAS DE SEGURANÇA, será responsável por controlar o recebimento da urna armazenadora de votos impressos, urna esta que terá a segurança física mantida por um lacre com

tecnologia de radio frequência.

Este equipamento, além de fazer um controle dos lacres radio frequência, vai auditar os votos impressos coletados pela urna, comparando o registro em texto às informações contidas nos códigos de
5 barras bidimensionais, verificando as assinaturas digitais através das respectivas chaves públicas geradas para os equipamentos coletores de voto, confirmando a procedência institucional e integridade do conteúdo do voto impresso.

Somente depois de auditado, o voto impresso será validado para o
10 escrutínio, e voltará a ser contabilizado de forma eletrônica a outros votos da seção eleitoral em um sistema simplificado de contabilidade de votos instalado também no EQUIPAMENTO DE AUDITORIA E APURAÇÃO DE VOTOS IMPRESSOS EM CÉDULAS DE SEGURANÇA.

Esta máquina também será responsável pela embalagem das cédulas
15 impressas coletadas em uma seção eleitoral, que sairão deste segundo equipamento, somadas e lacradas num invólucro plástico com outro chip de tecnologia radio frequência, dando início ao processo de armazenamento e auditoria controlado por esta tecnologia.

ESTADO DA TÉCNICA

20 Como é sabido historicamente, existem traumas culturais provocados pelo período em que o país realizava suas eleições em cédula de papel.

Muitas foram as fraudes ocorridas nesse longo período passado,

como por exemplo o “voto carreirinha”, quando um primeiro eleitor conseguia sair com a cédula virgem da sessão eleitoral, repassava para um corruptor que preenchia a cédula com o nome do seu candidato e entregava-a a um outro eleitor que inseria a cédula pré preenchida e repetia a operação de retirada de cédula virgem, fazendo assim um ciclo seguro, e evidentemente ilegal, para desvios de voto.

Registros de falsificação, adulteração, extravio de cédulas fazem parte de um tempo distante pois foram eficientemente extintos com o atual modelo eletrônico de votação. Portanto, a população em geral e também a classe política não acreditam na real necessidade da impressão do voto em papel.

No entanto aderem, de forma temerosa, ao voto totalmente eletrônico. Tal afirmação deve-se ao fato de que pesquisas científicas desenvolvidas por diferentes países que buscam melhorar a segurança e a transparência dos seus processos eletrônicos de votação, apontam, cada vez mais, para a necessidade de o eleitor, principalmente o eleitor leigo em tecnologia, ter a possibilidade de verificar se sua intenção de voto foi registrada e contabilizada corretamente sem correr riscos de extravios ocasionados por erros, que infelizmente estão presentes na votação totalmente eletrônica.

Diferentes estudos sobre voto eletrônico revelam a necessidade de existir uma trilha de auditoria física do voto individual, onde o eleitor, apenas com os olhos, possa ter garantias de que seu voto não sofrerá

qualquer possibilidade de adulteração ou extravio e assim, tendo certeza de que será somado ao resultado final da eleição.

Nesse contexto, surgiu no ano de 2.000, na tese de pós-doutorado proposta pela Ph.D. Rebecca Merccuri, intitulada “Electronic Vote
5 Tabulation – Checks & Balances”, o conceito “Voter-verified Paper Audit Trail (VVPAT)” e “Verified Paper Record (VPR)” que, em síntese, discorre sobre a importância da existência de auditoria em papel que venha permitir a recontagem dos votos de uma eleição eletrônica, quando assim for necessária.

10 Em 2006, o Ph.D. em criptologia Ronald Rivest, juntamente com o pesquisador do Instituto Nacional de Padrões e Tecnologia dos Estados Unidos, John Wack, idealizou o conceito “software independence” para os processos de votação eletrônica. Estes cientistas defendem que “*o sistema de votação é independente de software quando uma alteração ou um erro*
15 *imperceptível na programação dos sistemas de votação não provoca uma alteração ou erro, também imperceptíveis, no resultado das eleições (tradução nossa)”*.

Destaca-se também a norma técnica que está sendo aprimorada pelo Instituto de padrões e tecnologia (National Institute of Standards and
20 Technology - NIST) e pela Comissão de Assistência Eleitoral dos Estados Unidos da América, conhecida como “Voluntary Voting System Guidelines” que traz no rascunho da versão mais atual os seguintes requisitos mínimos para homologação de equipamentos de votação naquele

país (traduzidos para o português):

a - Ao menos dois registros do voto devem ser produzidos e um deles deve ser guardado em meio que não possa ser modificado pelo sistema (eletrônico) de votação, de forma que ambos os registros não estejam sob

5 controle de um único processo digital;

b) - O eleitor deve estar capacitado para verificar a igualdade dos dois registros do seu voto antes de deixar o local de votação;

c) O processo de verificação dos registros do voto deve ser independente e ao menos um deles deve ser conferível diretamente pelo
10 eleitor;

d) Os dois registros de um voto poderão ter sua consistência verificada posteriormente por meio de identificadores únicos que permitam a correlação dos registros.

No Brasil, destaca-se o artigo 5º da Lei Nº 12.034/94, que altera a
15 Lei dos Partidos Políticos (9.096/95), a Lei das Eleições (9.504/97) e o Código Eleitoral (4.737/65), que obriga o uso de dispositivos de impressão do voto a partir das eleições de 2014.

O artigo está suspenso por decisão liminar proferida na Ação Direta de Inconstitucionalidade nº 4547 interposta no Supremo Tribunal Federal
20 pela Procuradoria Geral da União. A ação questiona o voto impresso descrito na lei que, em tese, fere o direito ao sigilo do voto do eleitor.

Diante desse cenário, percebe-se que a urna eletrônica brasileira passou a não atender a legislação vigente, bem como os requisitos básicos

da norma norte-americana, por ser um coletor e apurador de votos do tipo *DRE* (de Direct Recording Electronic), caracterizada pela gravação eletrônica direta sem impressão do voto para conferência do eleitor.

OBJETIVO DA PATENTE

5 Os equipamentos, objetos desse presente pedido de patente de invenção, têm como objetivo exatamente a ampliação da segurança do processo eleitoral como um todo e foram pensados de uma forma onde as cédulas de votação impressas nos dispositivos serão manuseadas apenas e
tão somente pelo próprio eleitor, reduzindo assim o leque de
10 possibilidades de fraudes eleitorais que aconteciam principalmente no ato de apuração das cédulas de papel.

Para tanto, o modelo proposto é composto a partir de uma cédula de segurança, com o voto em texto e um segundo registro do voto em código de barras bidimensional, uma tecnologia de codificação de informações
15 para gráfico de barras cuja licença de uso é livre de royalties.

O voto em texto produzido para a cédula será gerada em um dispositivo de registro eletrônico do voto (Direct Recording Electronic - DRE), que inclusive poder ser a própria urna eletrônica hoje em uso, que será conectada, através de porta USB, ao EQUIPAMENTO DE
20 IMPRESSÃO E COLETA DE CÉDULAS DE SEGURANÇA DO VOTO.

Através do sistema, será possibilitado ao usuário a votação eletrônica que, após concluída, vai gerar o voto impresso, trazendo-lhe a certeza de sua escolha e impedindo que falhas nos equipamentos possam

extraviar o voto lançado de forma digital.

Explicado superficialmente, passam os dois equipamentos e os sistemas que os envolvem a serem melhor detalhados através dos desenhos anexos, pelos quais se vêem:

5 Figura 1 – mostra, à esquerda, o EQUIPAMENTO DE IMPRESSÃO E COLETA DE CÉDULAS DE SEGURANÇA DO VOTO conectado à um Tablet e, à direita, o mesmo equipamento conectado à Urna eletrônica;

 Figura 2 – mostra o EQUIPAMENTO DE IMPRESSÃO E COLETA DE CÉDULAS DE SEGURANÇA DO VOTO e, ao lado, detalhes
10 ampliados dos leitores biométricos;

 Figura 3 – mostra, em detalhe ampliado, as interfaces do EQUIPAMENTO DE IMPRESSÃO E COLETA DE CÉDULAS DE SEGURANÇA DO VOTO;

 Figura 4 - mostra a cédula de segurança do voto, com seus códigos
15 digitais;

 Figura 5 – mostra a urna independente sendo acoplada no EQUIPAMENTO DE AUDITORIA E APURAÇÃO DE VOTOS IMPRESSOS EM CÉDULAS DE SEGURANÇA;

 Figura 6 – mostra o EQUIPAMENTO DE AUDITORIA E
20 APURAÇÃO DE VOTOS IMPRESSOS EM CÉDULAS DE SEGURANÇA;

 Figura 7 - mostra o EQUIPAMENTO DE AUDITORIA E APURAÇÃO DE VOTOS IMPRESSOS EM CÉDULAS DE SEGURANÇA.
Nos detalhes, destacados, os dispositivos embaladores;

Figura 8 – mostra as cédulas lacradas, formando um bloco controlado por tecnologia RFID.

Em conformidade com os desenhos anexos, o “EQUIPAMENTO DE IMPRESSÃO E COLETA DE CÉDULAS DE SEGURANÇA DO VOTO”,
 5 um dos equipamentos objeto desse presente pedido de patente de invenção, constitui-se de um equipamento (1) envolto por cabine de votação (C) e que pode ser conectado à uma urna eletrônica (U), como mostra a figura 1, dito equipamento (1) em forma de computador com teclado reversível e tela sensível ao toque “touch screen” ou um “tablet” (2), com fone de
 10 ouvido (F), acoplado com câmera (3) com capacidade para realizar o reconhecimento biométrico da face do eleitor e conectado a um teclado mecânico (T) reaproveitado no processo de reciclagem das urnas.

O equipamento (1) possui uma bancada na qual é instalado um leitor biométrico de quatro dedos (4), um armazenador de cédulas virgens (5)
 15 conectado à sua impressora (6), alimentada também por bobina de papel (7), ambas comunicantes com uma saída (8) de impressora. A bancada possui também uma entrada (9) verificadora e coletora de cédulas impressas de voto confirmado pelo eleitor, além de uma entrada (10) verificadora e fragmentadora de cédula impressa porém rejeitada (anulada)
 20 pelo eleitor.

A entrada verificadora de cédulas impressas de voto confirmado pelo eleitor (9) é ligada à uma urna coletora independente (11) de cédulas confirmadas e verificadas pelo sistema, ao passo que a entrada

verificadora e fragmentadora de cédula impressa porém rejeitada pelo eleitor (10) é ligada à uma urna ecológica (12) receptora dos fragmentos dessas cédulas impressas porém rejeitadas pelos eleitores, formando assim o equipamento (1) propriamente dito, como mostram as figuras 1, 2 e 3.

5 O equipamento (1) de impressão e coleta de cédulas de segurança do voto é completado por um segundo “tablet” (13), onde estará instalado um software desenvolvido por uma entidade auditora do processo eleitoral, contendo as chaves públicas dos equipamentos. Este equipamento (13) será usado pelo eleitor para a verificação eletrônica do voto impresso em
10 código de barras bidimensional, possibilitando que o mesmo saia da sessão eleitoral após conferir os dois registros impressos do seu voto, sendo um em texto e o outro em código de barras bidimensional.

Assim constituído, o equipamento (1), integrado com software livre a ser desenvolvido, será utilizado como mesa receptora de votos para um
15 inédito sistema de coleta do voto eletrônico e do voto impresso em papel, com dupla identificação biométrica acionada pelo próprio eleitor.

O eleitor posiciona os quatro dedos da mão direita no leitor de identificação biométrica (4), quando o equipamento (1) faz então a coleta dos dados biométricos e envia uma solicitação assinada digitalmente para
20 o sistema eletrônico de votação instalado no computador ou “tablet” (2).

Em frente ao equipamento (1), o eleitor também é identificado através da câmera (3) que fará o reconhecimento biométrico da face.

Concluída a dupla identificação biométrica do eleitor, ele terá

acesso à interface de votação ou, no caso do eleitor analfabeto identificado previamente, acesso direto à interface especialmente desenvolvida para os eleitores sem instrução.

Através da tecla correspondente da tela (2), ou através do teclado mecânico reaproveitado da Urna Eletrônica (T), o eleitor escolhe seus candidatos, expondo as respectivas fotografias e demais informações possíveis. A fotografia do candidato é exposta na referida tela (2) para que o eleitor o reconheça sua escolha e confirme o voto digital.

Encerrada coleta do voto eletrônico, o eleitor autoriza, na tela (2) ou no teclado mecânico (T), a impressão de uma cédula de segurança (14) que será emitida pela saída (8) de impressora.

A cédula de segurança (14) do voto, mostrada pela figura 4, vai trazer as escolhas do eleitor para cada cargo em disputa naquela eleição e/ou plebiscito, explícitos em texto bastante legível. A cédula (14) também vai trazer o voto completo do eleitor codificado em código de barras bidimensional, que também vai conter assinaturas digitais da Justiça Eleitoral e de outra instituição auditora do processo (15).

Mais dois códigos de barras (16) e (17), de tamanho menor e capacidade de armazenamento reduzida, serão impressos na cédula (14) e trarão, cada um, uma assinatura digital, agora referente ao texto do voto impresso na cédula (14), produzidos pela Justiça Eleitoral e por outra entidade auditora do processo, respectivamente. A cédula (14) terá, ainda, código eletrônico em braile (18) para eleitor deficiente visual.

Com a cédula de segurança (14) impressa nas mãos, o eleitor poderá fazer a conferência também visual do voto codificado em barras no segundo “tablet” (13), que fará a leitura do código e exibirá na tela o registro do voto codificado.

5 Após confirmar que o texto e o registro do código estão, cada um, traduzindo sua intenção política, o eleitor insere a cédula (14) na entrada de confirmação de voto (9).

10 O equipamento (1) então lê, eletronicamente, o(s) código(s) de barras (16) ou (17) e (18) dessa cédula (14), extraíndo as assinaturas digitais institucionais.

15 Confirmado que aquela assinatura foi gerada pela chave privada emitida para a assinatura digital institucional, ou seja, após confirmada a procedência eletrônica da cédula (14), a mesma é sugada pelo dispositivo mecânico da entrada de confirmação de voto (9) e armazenada de forma aleatória na urna coletora independente (11). Essa verificação da assinatura evitará que o equipamento seja alimentado por cédulas não produzidas oficialmente.

20 Concluída a operação de coleta de voto, o equipamento (1) envia sinal digital para o sistema eleitoral gravar o registro digital do voto e encerrar a possibilidade de um novo voto para aquele eleitor. Dessa forma é computado normalmente o voto.

Caso o eleitor não concorde com a cédula impressa (14) do voto, desistindo ou percebendo que se enganou e pretendendo corrigir esse voto,

o eleitor vai inserir a referida cédula (14) na entrada (10) verificadora e fragmentadora de voto impresso rejeitado e, após o equipamento (1) confirmar a assinatura produzida pela chave privada das instituições e confirmada a procedência da cédula (14), a mesma é então sugada e triturada e os dejetos de papel serão armazenados na urna ecológica (12),
5 enviando um sinal para o sistema eleitoral instalado no computador do equipamento (1) cancelar o voto digital e reiniciar o processo de identificação do eleitor, retornando todo o processo de votação ao estágio inicial.

10 Com isso é possibilitada a correção do voto impresso pelo próprio eleitor. Nesse caso, o voto rejeitado não é computado no banco de dados do sistema, evitando contagem errada ao final da votação e permitindo que o eleitor tenha nova chance ou opção de votar, sem contaminar todo o processo com cédulas rejeitadas pelos eleitores.

15 Caso o eleitor seja analfabeto, o mesmo poderá votar utilizando santinhos com código de barras bidimensional previamente distribuídos pelos candidatos.

Após a dupla identificação biométrica, o eleitor analfabeto em posse desse material publicitário impresso pelos candidatos com código
20 de barras bidimensional, vai inserir o santinho na entrada (10) verificadora trituradora, visualizando a foto de seu candidato na tela (2), repetindo a operação até o final do processo, quando será impressa a cédula (14) de segurança a ser confirmada imediatamente pelo eleitor sem instrução, que

devera ser orientado a inserir a cédula (14) do voto na entrada de confirmação de voto (9).

O mesmo procedimento de leitura de santinhos poderá ser utilizado para auxílio ao voto dos eleitores com deficiência visual, porém, ao invés
5 de confirmar o voto apresentado na tela (2), o eleitor deficiente visual confirmará seu voto digital através de um fone de ouvido (F), que repassará as instruções de manuseio do equipamento (1) para confirmação do voto, instruindo o eleitor deficiente até o completo processo do voto digital e destinação do voto impresso, que também será transcrito pelo
10 código em Braille (18), na interface verificadora coletora (9). O eleitor deficiente visual também poderá inserir o voto através do teclado mecânico (T), que está conectado ao equipamento (1).

Em todas as situações em que voto impresso é confirmado, o eleitor poderá imprimir, ao final do processo, um comprovante de
15 comparecimento, oriundo da bobina de papel (7) instalada na parte inferior do equipamento (1), que será fornecida através da saída (8) da impressora.

Como se observa, pelo sistema proposto é eliminada a figura do mesário.

Após o encerramento da votação, urna coletora independente (11)
20 de cédulas confirmadas, ou seja, de voto confirmado, é então sacada do equipamento de votação (1) e levada para o ambiente de auditoria, escrutínio e totalização dos votos, conforme mostra a figura 5.

Nesse outro ambiente, a urna coletora independente (11) de cédulas

confirmadas é acoplada, como mostra a figura 5, no EQUIPAMENTO DE AUDITORIA E APURAÇÃO DE VOTOS IMPRESSOS EM CÉDULAS DE SEGURANÇA (19), quando então é iniciado o processo de auditoria e contabilidade dos votos.

5 Este equipamento (19), também objeto da presente patente, como é mostrado em especial pelas figuras 6 e 7 e também pela figura 5, é composto, em uma de suas laterais, por uma entrada (20) de urna coletora independente (11), dispositivo de leitura/gravação de RFID (21) e uma entrada de cédulas auditadas (22). Na outra lateral possui impressora (23)
10 e monitor LCD (24), reaproveitado das Urnas Eletrônicas.

No interior, o equipamento (19) possui um leitor ótico de OCR e QR code e uma CPU (25) e dispositivos embaladores (26), comunicantes, na outra lateral, com uma saída (27) de cédulas embaladas que receberão uma identificação RFID a ser aplicada pelo etiquetador (28).

15 O equipamento (19) será alimentado pelas informações trazidas na urna armazenadora independente (11), ou pelas cédulas de segurança impressas (14) com lacre, em um processo de auditoria, tendo diferentes funções exercidas numa mesma rotina automatizada mecanicamente.

Caso o lacre da urna coletora independente (11) de confirmação de
20 voto tenha indícios de violação, o equipamento (19) emite aviso sonoro e em texto no LCD, sendo a referida urna coletora independente (11) remetida para comissão apuradora, que decidirá sobre o prosseguimento ou não de sua apuração.

A primeira função do EQUIPAMENTO DE AUDITORIA E APURAÇÃO DE VOTOS IMPRESSOS EM CÉDULAS DE SEGURANÇA (19) é receber a urna coletora independente (11) pela entrada (20) e verificar a procedência do lacre da urna coletora independente (11) através do dispositivo (21) rádio frequência e, confirmada a relação entre o chip e a seção eleitoral, os votos impressos são automaticamente retirados da referida urna coletora independente (11).

As cédulas (14) passam então pelo leitor ótico (25), que fará a leitura dos códigos de barras (16), (17) ou (18), extraíndo e verificando as assinaturas digitais, e comparando às informações do voto em texto às informações do voto codificado em código de barras.

Após auditoria comparativa, o voto impresso é então contabilizado eletronicamente e enviado para um módulo (26) onde, junto com as demais cédulas (14) da seção eleitoral em escrutínio, serão armazenadas. Concluída a apuração total dos votos, as cédulas sairão lacradas em plástico e enviados para saída (27), formando um bloco de papel (29), como mostra a figura 8, que receberá, na etiquetadora (28), um chip de rádio frequência, concluindo assim o processo de auditoria e escrutínio eletrônica das cédulas impressas.

A entrada de votos em auditoria (22), receberá as cédulas que necessitaram de outro processo de inspeção. O procedimento de apuração de cédulas auditadas é similar ao procedimento de cédulas coletadas, diferenciando apenas na origem das informações de identificação rádio

frequência, ou seja, ao invés de ler o lacre RFID da urna independente, a interface fará a leitura de um identificador RFID de um bloco de cédulas onde se detectou a necessidade de uma auditoria mais refinada.

Para efeito de segurança, o EQUIPAMENTO DE AUDITORIA E
5 APURAÇÃO DE VOTOS IMPRESSOS EM CÉDULAS DE SEGURANÇA
(19) é desprovido de dispositivo de entrada, possuindo somente o disco armazenador dos programas de controle dos engenhos mecatrônicos e de interpretação, auditoria e contabilidade de votos impressos.

Relatórios, alertas e o boletim de totalização serão todos emitidos
10 em texto e código de barras bidimensional através da impressora e registrados no arquivo de log da máquina.

Têm-se como objetivo que este segundo equipamento da presente patente seja fabricado utilizando componentes eletrônicos como processadores, memória, impressora, tela LCD e os componentes plásticos
15 reaproveitados do processo de reciclagem das urnas eletrônicas atuais, que serão substituídas por computadores ou tablets no amadurecer do processo de implantação dos novos equipamentos de votação eletrônica e mecânica objetos desta patente.

REIVINDICAÇÕES

1) “EQUIPAMENTO DE IMPRESSÃO E COLETA DE CÉDULAS DE SEGURANÇA DO VOTO”, sendo um equipamento (1) envolto por cabine de votação (C) passível de conexão à urna eletrônica (U), **caracterizado**

5 por configuração de computador com teclado reversível com tela “touch screen” ou “tablet” (2), fone de ouvido (F), câmera (3) de reconhecimento biométrico da face do eleitor e conectado a teclado mecânico (T), dito equipamento (1) dotado, também, de bancada com leitor biométrico de quatro dedos (4), armazenador de cédulas virgens (5) conectado à

10 impressora (6) alimentada por bobina de papel (7), ambas comunicantes com uma saída (8) de impressora, dita bancada possuindo, ainda, entrada (9) verificadora e coletora de cédulas impressas de voto confirmado pelo eleitor, além de uma entrada (10) verificadora e fragmentadora de cédula impressa porém rejeitada (anulada) pelo eleitor, sendo a referida entrada

15 (9) ligada à uma urna coletora independente (11) de cédulas confirmadas e verificadas pelo sistema e, a entrada (10) ligada à uma urna ecológica (12) receptora dos fragmentos dessas cédulas impressas porém rejeitadas pelos eleitores, dito equipamento (1) completado por um segundo “tablet” (13), instalado com software desenvolvido por uma entidade auditora do

20 processo eleitoral, contendo as chaves públicas dos equipamentos, para verificação eletrônica (pelo próprio eleitor), do voto impresso em código de barras bidimensional.

2) “EQUIPAMENTO DE IMPRESSÃO E COLETA DE CÉDULAS DE

SEGURANÇA DO VOTO”, de acordo com reivindicação 1, o equipamento (1), de uso com mesa receptora de votos, formar um sistema **caracterizado** pela coleta do voto eletrônico e de voto impresso em papel, com dupla identificação biométrica, em acionamento pelo próprio eleitor.

5 3) “EQUIPAMENTO DE IMPRESSÃO E COLETA DE CÉDULAS DE SEGURANÇA DO VOTO”, de acordo com reivindicação 2, **caracterizado** por, após manuseado o teclado pelo eleitor, ser produzida (3) cédula impressa (14) com voto completo codificado em código de barras bidimensional, com assinaturas digitais da Justiça Eleitoral e de outra
10 instituição auditora do processo (15), além de códigos de barras (16) e (17), de tamanho menor e capacidade de armazenamento reduzida e, ainda, código eletrônico em braile (18).

4) “EQUIPAMENTO DE IMPRESSÃO E COLETA DE CÉDULAS DE SEGURANÇA DO VOTO”, de acordo com reivindicação 2, ocorrer
15 conferência eletrônica pelo equipamento (1) e também pelo segundo “tablet” (13), **caracterizado** pela cédula (14) ser inserida na entrada de confirmação de voto (9) e armazenada de forma aleatória na urna coletora independente (11), com envio de sinal digital para gravação do registro digital do voto pelo sistema eleitoral.

20 5) “EQUIPAMENTO DE IMPRESSÃO E COLETA DE CÉDULAS DE SEGURANÇA DO VOTO”, de acordo com reivindicação 2, em caso de correção de voto, **caracterizado** pela inserção da cédula (14) na entrada (10) para trituração e envio de sinal digital para o sistema eleitoral, para

cancelamento de voto, sem ser computado, e reinício do processo de votação.

6) “EQUIPAMENTO DE IMPRESSÃO E COLETA DE CÉDULAS DE SEGURANÇA DO VOTO”, de acordo com reivindicação 2, em caso de

5 leitor de analfabeto, **caracterizado** pelo uso de santinhos com código de barras bidimensional com dupla identificação biométrica, seguindo-se a inserção na entrada (10) verificadora trituradora, visualizando a foto de seu candidato na tela (2), repetindo a operação até o final do processo, para impressão da cédula (14) e confirmação pela entrada de confirmação
10 de voto (9).

7) “EQUIPAMENTO DE IMPRESSÃO E COLETA DE CÉDULAS DE SEGURANÇA DO VOTO”, de acordo com reivindicação 2, em caso de

eleitores com deficiência visual, **caracterizado** pelo lançamento do voto através de santinhos com códigos de barras ou através do teclado mecânico
15 (T), e confirmação do voto através do fone de ouvido (F), inserindo a cédula (14) com o voto transcrito em código Braille (18) na entrada coletora (9) ou na entrada trituradora (10).

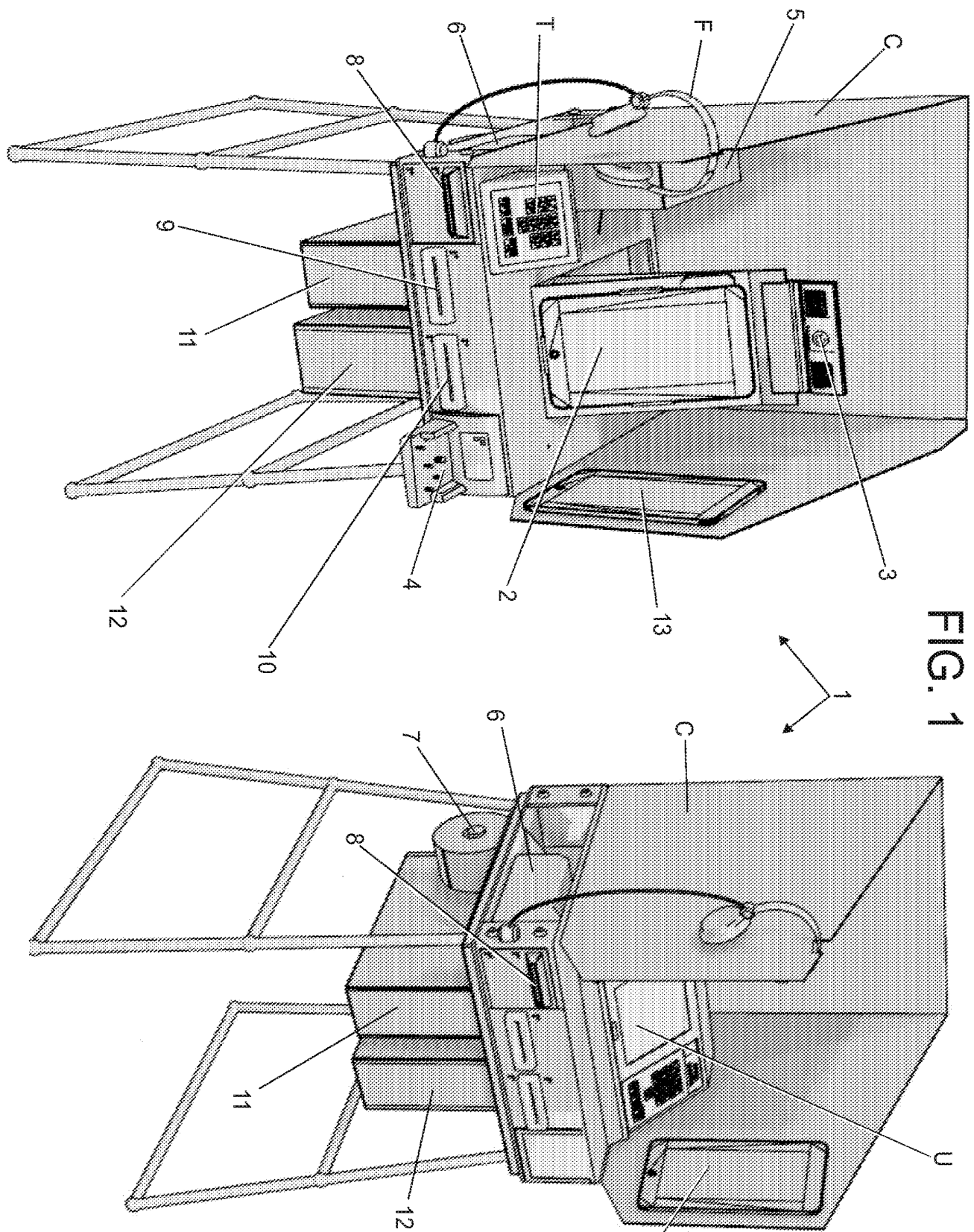
8) “EQUIPAMENTO DE IMPRESSÃO E COLETA DE CÉDULAS DE SEGURANÇA DO VOTO” de acordo com reivindicação 2, após emissão

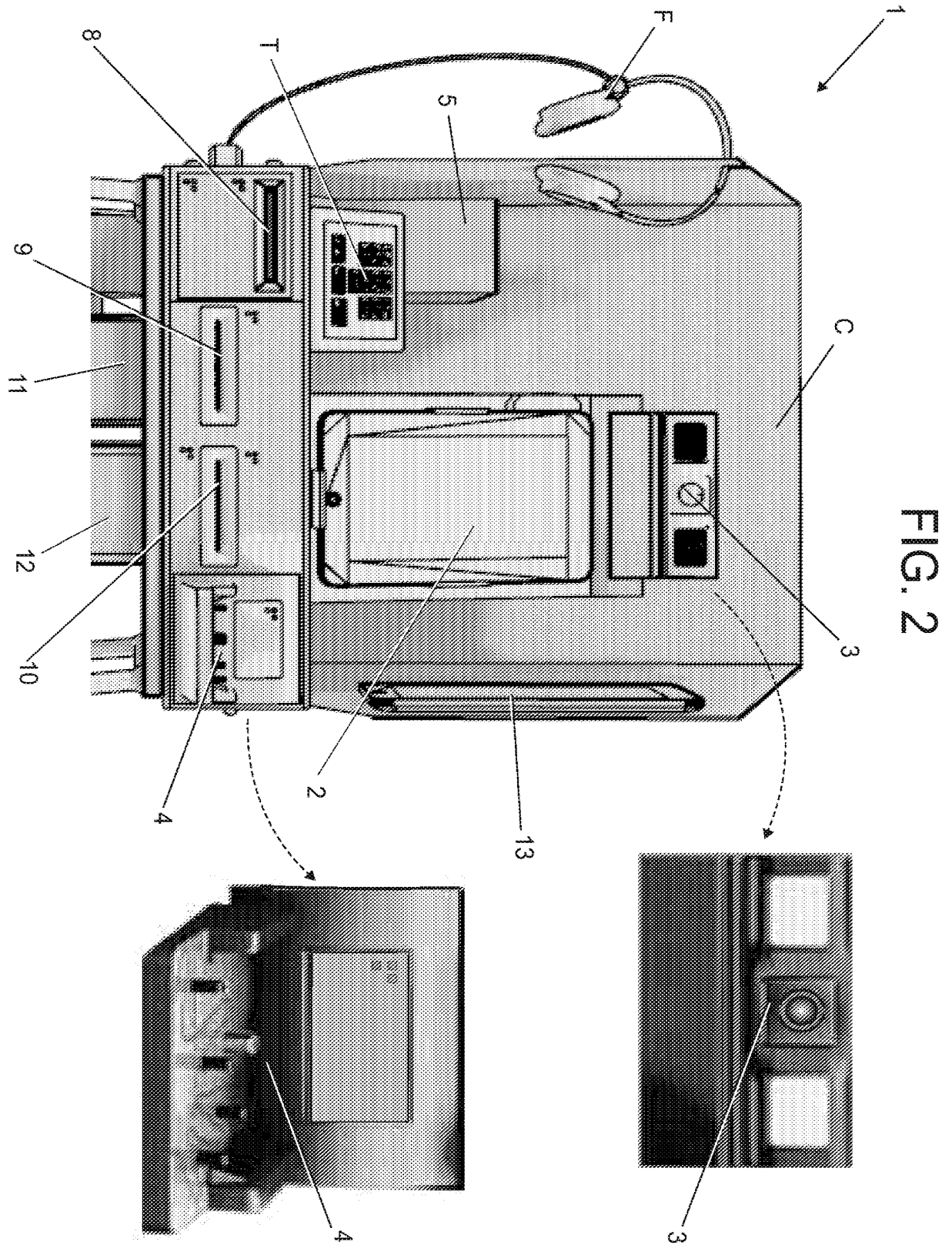
20 de comprovante de voto através de saída (8) da impressora, **caracterizado** pela urna coletora independente (11) com as cédulas (14) armazenadas, ser retirada e introduzida na entrada (20) do EQUIPAMENTO DE AUDITORIA E APURAÇÃO DE VOTOS IMPRESSOS EM CÉDULAS DE

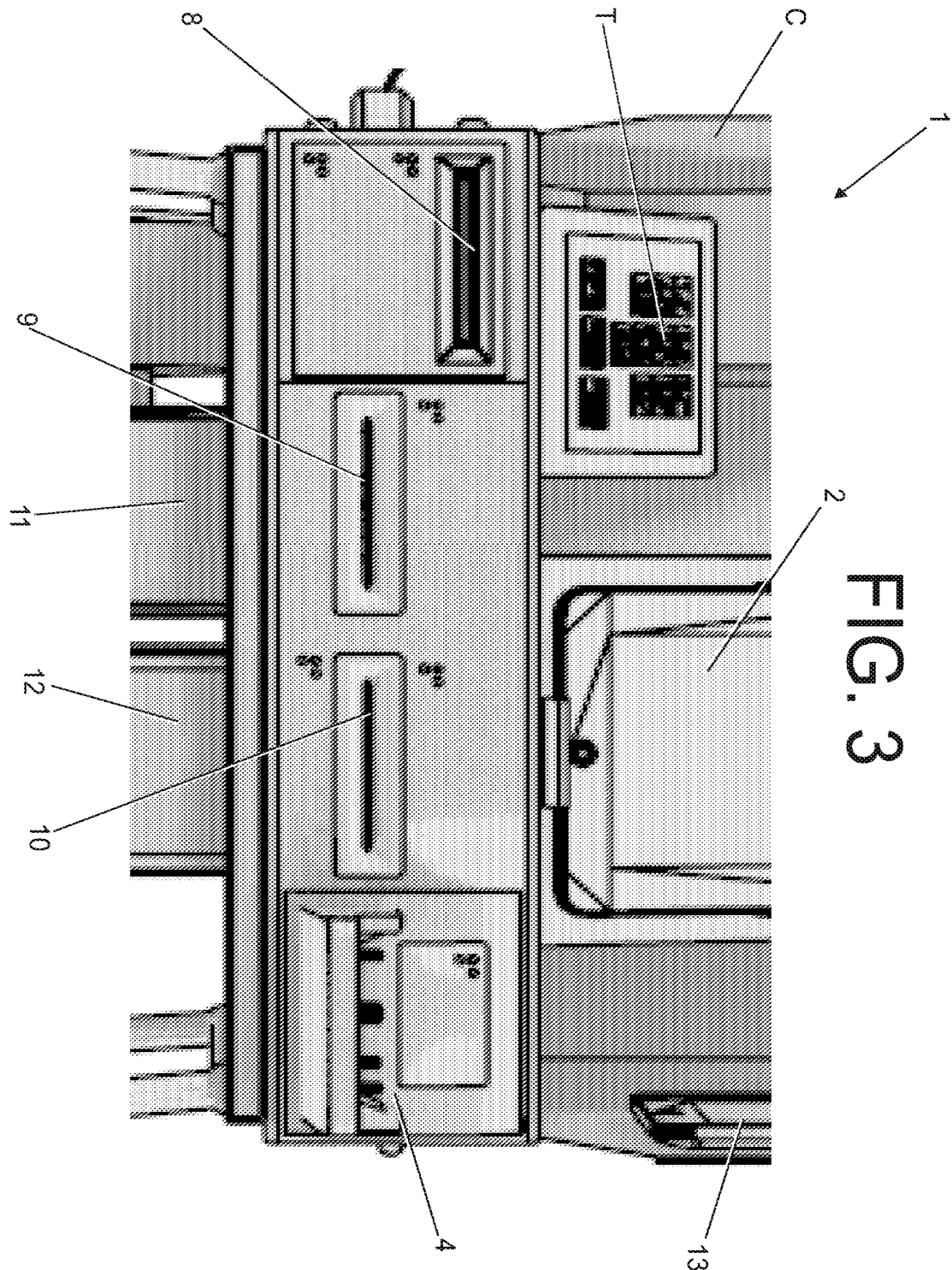
SEGURANÇA dotado também de leitor/gravador de RFID (21), entrada de
cédulas auditadas (22) possuindo, na outra lateral, impressora (23) e
monitor LCD (24) e, em seu interior, um leitor ótico de OCR e QR code e
uma CPU (25) e dispositivos embaladores (26), comunicantes, na outra
5 lateral, com uma saída (27) de cédulas embaladas, passíveis de receber
identificação RFID por etiquetador (28).

9) “EQUIPAMENTO DE AUDITORIA E APURAÇÃO DE VOTOS
IMPRESSOS EM CÉDULAS DE SEGURANÇA”, de acordo com
reivindicações 2 e 8, formar um sistema **caracterizado** por ler as
10 informações trazidas na urna coletora independente (11) através do
dispositivo (21) rádio frequência e, caso hajam indícios de violação, ser
emitido aviso sonoro e em texto no LCD, para reavaliações eleitorais.

10) “EQUIPAMENTO DE AUDITORIA E APURAÇÃO DE VOTOS
IMPRESSOS EM CÉDULAS DE SEGURANÇA”, de acordo com
15 reivindicação 9, **caracterizado** pela leitura dos códigos de barras (16),
(17) ou (18), e contabilização eletrônica das cédulas (14), armazenadas no
módulo (26), seguindo-se o lacre, formando um bloco (29) expulso pela
saída (27), recebendo, na etiquetadora (28), um chip de rádio frequência,
de uso com mesa receptora de votos, formar um sistema **caracterizado**
20 pela coleta do voto eletrônico e de voto impresso em papel, com dupla
identificação biométrica, em acionamento pelo próprio eleitor.







Π
G
Ω

FIG. 4

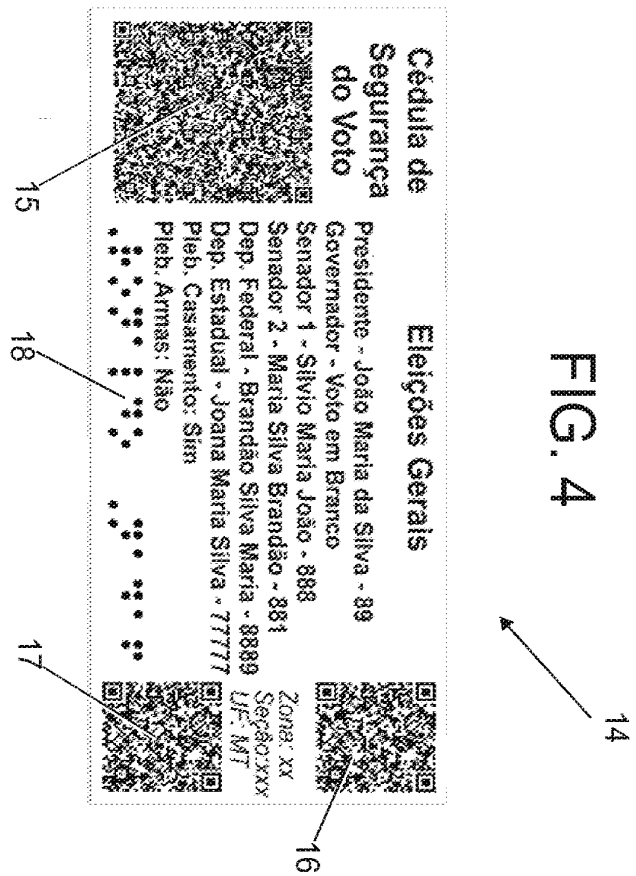
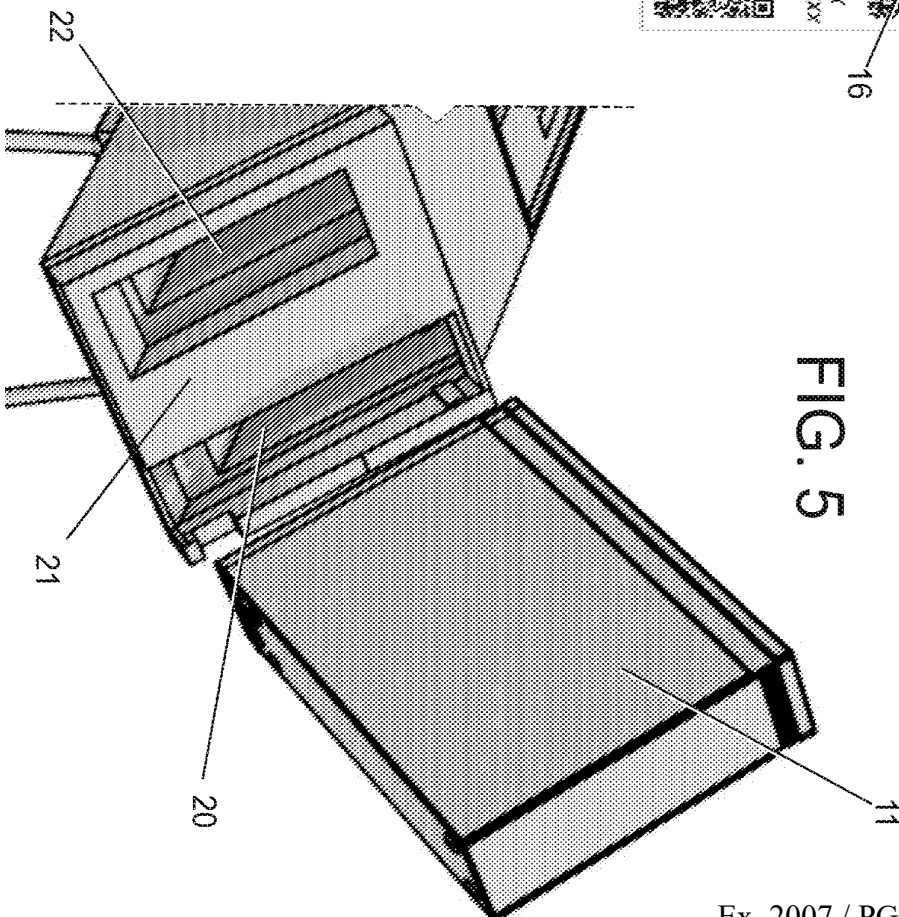
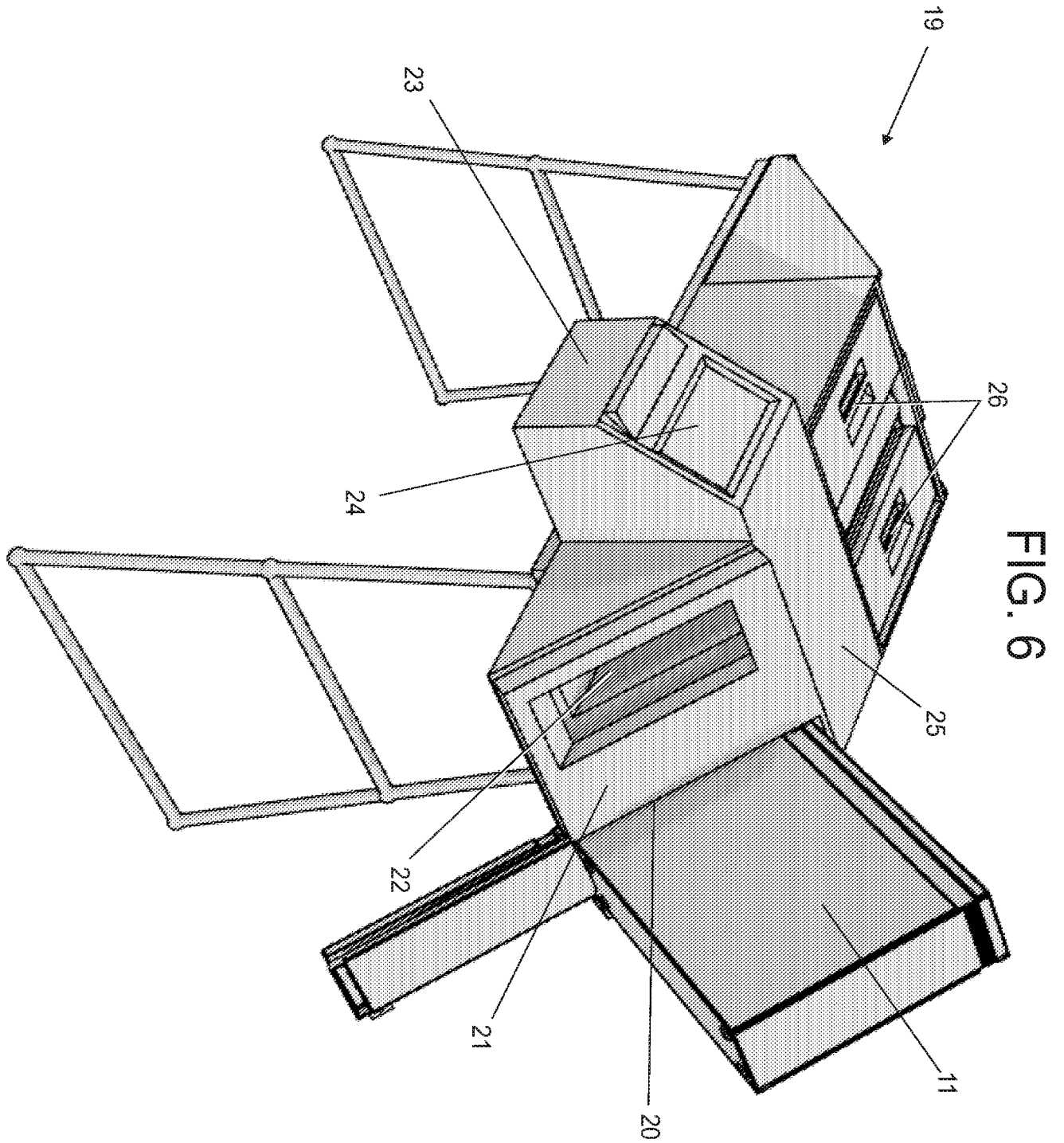
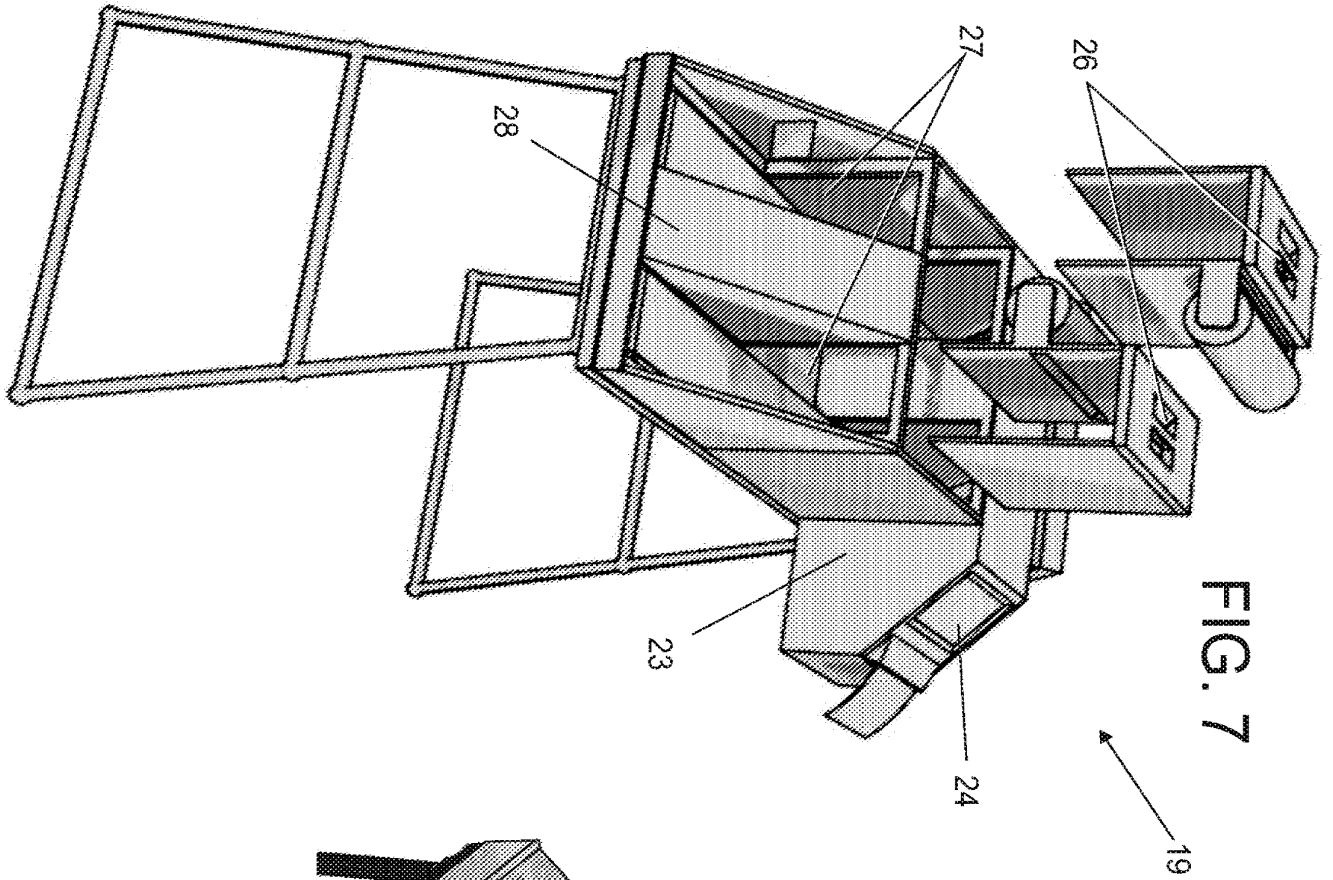
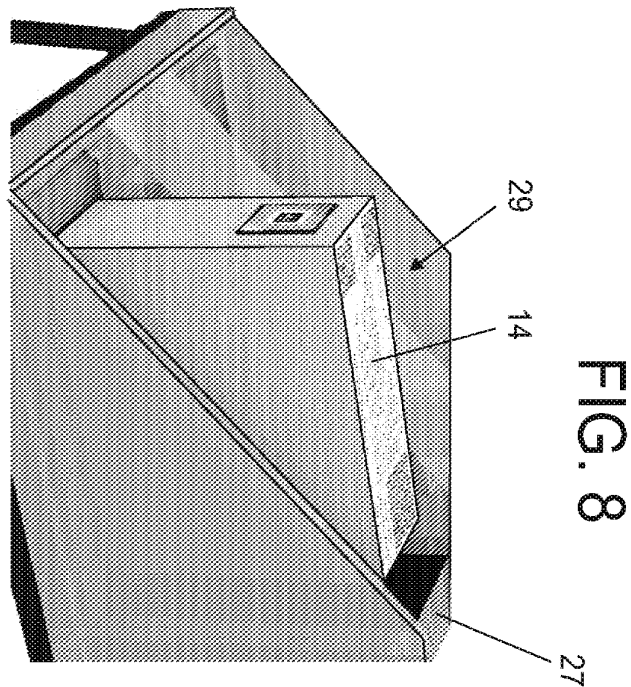


FIG. 5







RESUMO

“EQUIPAMENTO DE IMPRESSÃO E COLETA DE CÉDULAS DE
SEGURANÇA DO VOTO E EQUIPAMENTO DE AUDITORIA E
APURAÇÃO DE VOTOS IMPRESSOS EM CÉDULAS DE SEGURANÇA,
5 PARA MODELO DE VOTAÇÃO MECATRÔNICA”, onde um equipamento
(1) forma um sistema que possibilita ao próprio eleitor, votar e obter uma
cédula de impressão (14) pela qual serão confirmados, o voto eletrônico e
a impressão, através de códigos de barra (15), (16), (17) e (18) nela
gravados. Tal cédula (13) é transferida para um segundo equipamento (19),
10 de apuração de votos, onde tais informações serão lidas, formando um
sistema de armazenamento eletrônico e impresso, em total interação e
passível de ser auditado, caso haja dúvidas em relação a fraudes,
trazendo total segurança ao sistema eleitoral.

Electronic Acknowledgement Receipt

EFS ID:	38922848
Application Number:	16745621
International Application Number:	
Confirmation Number:	6960
Title of Invention:	Optical Character Recognition Of Voter Selections For Cast Vote Records
First Named Inventor/Applicant Name:	James M. Canter
Customer Number:	36275
Filer:	Richard D. Egan/Marty Jones
Filer Authorized By:	Richard D. Egan
Attorney Docket Number:	HART:032C2
Receipt Date:	20-MAR-2020
Filing Date:	17-JAN-2020
Time Stamp:	11:37:08
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	IDS_3.pdf	1035204	no	4
			c62d799952630cae73aa09e2fecad50298424a9e4		

Warnings:

Information:					
A U.S. Patent Number Citation or a U.S. Publication Number Citation is required in the Information Disclosure Statement (IDS) form for autoloading of data into USPTO systems. You may remove the form to add the required data in order to correct the Informational Message if you are citing U.S. References. If you chose not to include U.S. References, the image of the form will be processed and be made available within the Image File Wrapper (IFW) system. However, no data will be extracted from this form. Any additional data such as Foreign Patent Documents or Non Patent Literature will be manually reviewed and keyed into USPTO systems.					
2	Foreign Reference	B1.pdf	4124779 24069df825c5d61804f89090fa19fb12f5f87467	no	29
Warnings:					
Information:					
3	Non Patent Literature	C1.pdf	994970 496851d106eb0ea702f31c096ed95c7fe2409802	no	99
Warnings:					
Information:					
4	Non Patent Literature	C2.pdf	22141203 d3931d9306d13907631ee956e172606c5ef3af95	no	100
Warnings:					
Information:					
5	Non Patent Literature	C3.pdf	2342016 8f56063ebe1e90d45835372b80f79da6fd5fb18c	no	175
Warnings:					
Information:					
6	Non Patent Literature	C4.pdf	1851137 53c02a35fe702e455f64062578986b3d18d4ef13	no	3
Warnings:					
Information:					
7	Non Patent Literature	C5.pdf	12303301 64e1923904c0adad9c3536635da04b1e44046c57	no	172
Warnings:					
Information:					
Total Files Size (in bytes):			44792610		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		16745621
	Filing Date		2020-01-17
	First Named Inventor	JAMES M. CANTER	
	Art Unit		
	Examiner Name		
	Attorney Docket Number		HART:032C2

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	7306148		2007-12-11	Morganstein	
	2	5377099		1994-12-27	Miyagawa	
	3	6885758		2005-04-26	Bayer	
	4	5726435		1998-03-10	Hara et al.	
	5	2612994		1949-10-20	Woodland et al.	
	6	10147259		2018-12-04	Dvorak	
	7	10002481		2018-06-19	Seibel et al.	
	8	9165417		2015-10-20	Valles Fontanals et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number		16745621
Filing Date		2020-01-17
First Named Inventor	JAMES M. CANTER	
Art Unit		
Examiner Name		
Attorney Docket Number	HART:032C2	

9	6873966		2005-03-29	Babbitt et al.	
10	7729991		2010-06-01	Rodriguez et al.	
11	RE40449		2008-08-05	Provitola et al.	
12	6250548		2001-06-26	McClure et al.	
13	5764799		1998-06-09	Hong et al.	
14	9361531		2016-06-07	Stella	
15	3609685		1971-09-28	Deutsch	
16	9401059		2016-07-26	Backert et al.	
17	6971574		2005-12-06	Herskowitz	
18	7080779		2006-07-25	Cummings	
19	7406201		2008-07-29	Heilper et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16745621
Filing Date	2020-01-17
First Named Inventor	JAMES M. CANTER
Art Unit	
Examiner Name	
Attorney Docket Number	HART:032C2

If you wish to add additional U.S. Patent citation information please click the Add button. [Add](#)

U.S.PATENT APPLICATION PUBLICATIONS [Remove](#)

Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20190213820		2019-07-11	Sebes et al.	
	2	20090166417		2009-07-02	Dammann et al.	
	3	20060041468		2006-02-23	Reardon	
	4	20140012635		2014-01-09	Joyce et al.	
	5	20100114674		2010-05-06	Daza Fernandez et al.	
	6	20110202464		2011-08-18	Carbullido	
	7	20180102013		2018-04-12	Spanos et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. [Add](#)

FOREIGN PATENT DOCUMENTS [Remove](#)

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵
-------------------	---------	--------------------------------------	---------------------------	------------------------	------------------	---	--	----------------

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16745621
Filing Date	2020-01-17
First Named Inventor	JAMES M. CANTER
Art Unit	
Examiner Name	
Attorney Docket Number	HART:032C2

1	0120562A2	WO		2001-03-22	Adler et al.		
2	2004038632	WO		2004-05-06	Boldin		
3	1020130185582	BR		2014-09-02	Nadaf		

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	Kim et al., "Improved Support For Machine-Assisted Ballot-Level Audits", Usenix Journal Of Election Technology And Systems (JETS), Vol. 1, No. 1, August 2013, 18 pgs.	
	2	Keller et al., "A PC-Based Open-Source Voting Machine With An Accessible Voter-Verifiable Paper Ballot", Usenix, 2005, 12 pgs.	
	3	Mohapatra et al., "Spell Checker For OCR", International Journal Of Computer Science And Information Technologies", Vol. 4, No. 1, 2013, 7 pgs.	
	4	Bunke, "A Fast Algorithm For Finding The Nearest Neighbor Of A Word In A Dictionary", IAM-93-025, November 1993, 16 pgs.	
	5	Hassan et al., "Language Independent Text Correction Using Finite State Automata", IBM Cairo Technology Development Center, 2008, 6 pgs.	
	6	Toledo, "Election Tally Sheets Processing System", IAPR Workshop, 2016, 5 pgs.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number		16745621
Filing Date		2020-01-17
First Named Inventor	JAMES M. CANTER	
Art Unit		
Examiner Name		
Attorney Docket Number	HART:032C2	

7	Ashford, "QR Codes And Academic Libraries: Reaching Mobile Users", Faculty Publications- George Fox University Libraries, 2010, 6 pgs.
8	Barrera, "Optical Encryption And QR Codes: Secure And Noise-Free Information Retrieval", Optics Express, 2013, 6 pgs.
9	Krawczyk et al., "HMAC: Keyed-Hashing For Message Authentication", Network Working Group, February 1997, 11 pgs.
10	Essex et al., "Hover: Trustworthy Elections With Hash-Only Verification", IEEE Computer And Reliability Societies, 2012, 7 pgs.
11	Preneel, "The First 30 Years Of Cryptographic Hash Functions And The NIST SHA-3 Competition", Katholieke Universiteit Leuven and IBBT, Dept. Electrical Engineering, 2010, 15 pgs.
12	Shamos, "Electronic Voting Glossary", Carnegie Mellon University, 2011, 8 pgs.

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16745621
Filing Date	2020-01-17
First Named Inventor	JAMES M. CANTER
Art Unit	
Examiner Name	
Attorney Docket Number	HART:032C2

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Richard D. Egan/	Date (YYYY-MM-DD)	2020-03-17
Name/Print	Richard D. Egan	Registration Number	36788

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	38885403
Application Number:	16745621
International Application Number:	
Confirmation Number:	6960
Title of Invention:	Optical Character Recognition Of Voter Selections For Cast Vote Records
First Named Inventor/Applicant Name:	James M. Canter
Customer Number:	36275
Filer:	Richard D. Egan/Marty Jones
Filer Authorized By:	Richard D. Egan
Attorney Docket Number:	HART:032C2
Receipt Date:	17-MAR-2020
Filing Date:	17-JAN-2020
Time Stamp:	11:29:59
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	IDS_2.pdf	1036903	no	7
			73c171f89b5f4f0cd065208ac415cfa3e6d371a8		

Warnings:

Information:					
2	Non Patent Literature	C1.pdf	4019683	no	18
			6359e577d1a63387afc17c07063d2dfc04b1daa7		
Warnings:					
Information:					
3	Non Patent Literature	C5.pdf	3049191	no	6
			a3fc446894abeb18928e9be671d0d85a90677bb5		
Warnings:					
Information:					
4	Non Patent Literature	C6.pdf	4035115	no	5
			805797f779ae84ec016301b737c4db6dabafcf471		
Warnings:					
Information:					
5	Non Patent Literature	C7.pdf	3689320	no	6
			38eacd23df6d6f67eac54573ec28da55525fe0e6		
Warnings:					
Information:					
6	Non Patent Literature	C8.pdf	3204748	no	6
			3b7e145b6d3425f49d4622b6f99f362074408c6e		
Warnings:					
Information:					
7	Non Patent Literature	C9.pdf	2183658	no	11
			09d0709c3e69bcee014aaaa880e8715fd0f48474		
Warnings:					
Information:					
8	Non Patent Literature	C10.pdf	2837218	no	7
			371b5e3e320f6b9d900a09e6de4cfbde1b682665		
Warnings:					
Information:					

Ex: 2007 / PCB2025-00066 / Page 501 of 555

9	Non Patent Literature	C11.pdf	1725916	no	15
			5abd0c16c027466b2d207dcd53ac8759b9d283f		
Warnings:					
Information:					
10	Non Patent Literature	C12.pdf	876592	no	8
			efe7d6dd91fb1fab93a2fddca9230bc771cd460		
Warnings:					
Information:					
11	Non Patent Literature	C2.pdf	589610	no	12
			063f8aa6881d072d78a0786976d37b64acd69196		
Warnings:					
Information:					
12	Non Patent Literature	C3.pdf	1106578	no	7
			d38838717ee840d7f513e847d949db7c0a14a2bf		
Warnings:					
Information:					
13	Non Patent Literature	C4.pdf	338094	no	16
			0b28153d05459d9e2b3a8a016522941f476a6cca		
Warnings:					
Information:					
14	Foreign Reference	B1.pdf	8642415	no	75
			624d668e8f886f33a5fdd42bdfdea74d8eea2e018		
Warnings:					
Information:					
15	Foreign Reference	B2.pdf	6681697	no	77
			ce05d9d0fc543cac5d3783e699dd2b450869ecd7		
Warnings:					
Information:					

16	Foreign Reference	B3.pdf	25265615	no	158
			dd4e74ac157cd3d8b3213d56ab0f1d64cbca65d0		
Warnings:					
Information:					
Total Files Size (in bytes):				69282353	
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875						Application or Docket Number 16/745,621				
APPLICATION AS FILED - PART I										
(Column 1)		(Column 2)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY				
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)		RATE(\$)	FEE(\$)			
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	300			
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A			N/A	660			
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	760			
TOTAL CLAIMS (37 CFR 1.16(j))	22 minus 20 =	*				x 100 =	200			
INDEPENDENT CLAIMS (37 CFR 1.16(h))	1 minus 3 =	*				x 460 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL		TOTAL	1920			
APPLICATION AS AMENDED - PART II										
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY		
AMENDMENT A		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x =			x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =			x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
						TOTAL ADD'L FEE			TOTAL ADD'L FEE	
AMENDMENT B		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x =			x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =			x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
						TOTAL ADD'L FEE			TOTAL ADD'L FEE	
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.										



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	TOT CLAIMS	IND CLAIMS
16/745,621	01/17/2020	2876	1920	HART:032C2	22	1

CONFIRMATION NO. 6960

FILING RECEIPT



000000011457787

36275

Egan, Peterman, Enders & Huston LLP.
1101 S. Capital of Texas Highway
Bldg C, Suite 200
Austin, TX 78746

Date Mailed: 02/05/2020

Receipt is acknowledged of this non-provisional utility patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF FIRST INVENTOR, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection.

Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections provided that the request is grantable.

Inventor(s)

James M. Canter, Austin, TX;
Drew E. Tinney, Austin, TX;
Ievgen Konovalenko, Austin, TX;

Applicant(s)

Hart InterCivic, Inc., Austin, TX;

Power of Attorney: The patent practitioners associated with Customer Number 36275

Domestic Priority data as claimed by applicant

This application is a CON of 16/560,222 09/04/2019 PAT 10573111
which is a CON of 16/239,607 01/04/2019 PAT 10445966
which claims benefit of 62/711,212 07/27/2018

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see <http://www.uspto.gov> for more information.) - None.

Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 02/04/2020

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 16/745,621**

Projected Publication Date: 05/14/2020

Non-Publication Request: No

Early Publication Request: No
Title

Optical Character Recognition Of Voter Selections For Cast Vote Records

Preliminary Class

235

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific

page 2 of 4

countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER
Title 35, United States Code, Section 184
Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop

technology, manufacture products, deliver services, and grow your business, visit <http://www.SelectUSA.gov> or call +1-202-482-6800.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		16745621
	Filing Date		2020-01-17
	First Named Inventor	JAMES M. CANTER	
	Art Unit		
	Examiner Name		
	Attorney Docket Number	HART:032C2	

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	7635088		2009-12-22	Kevin Chung et al.	
	2	7988047		2011-08-02	Kevin Chung et al.	
	3	8261986		2012-09-11	Kevin Chung et al.	
	4	8991701		2015-03-31	Steve Bolton et al.	
	5	5497318		1996-03-05	Takayoshi Miyagawa et al.	
	6	10445966		2019-10-15	Canter et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16745621
Filing Date	2020-01-17
First Named Inventor	JAMES M. CANTER
Art Unit	
Examiner Name	
Attorney Docket Number	HART:032C2

1	20090289115	2009-11-26	Kevin Chung et al.
2	20180350180	2018-12-06	Daniel Onischuk
3	20170344538	2017-11-30	Hiroya Horai
4	20140231513	2014-08-21	Sean Brockhouse et al.
5	20020084325	2002-07-04	David C. Reardon
6	20090256703	2009-10-15	Steve Bolton
7	20050269406	2005-12-08	Andrew C. Neff

If you wish to add additional U.S. Published Application citation information please click the Add button. [Add](#)

FOREIGN PATENT DOCUMENTS

[Remove](#)

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² i	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	2012175758	WO		2012-12-27	Indra Sistemas, S.A.		

If you wish to add additional Foreign Patent Document citation information please click the Add button. [Add](#)

NON-PATENT LITERATURE DOCUMENTS

[Remove](#)

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		16745621
	Filing Date		2020-01-17
	First Named Inventor	JAMES M. CANTER	
	Art Unit		
	Examiner Name		
	Attorney Docket Number	HART:032C2	

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	Quesenbery, Making Voting Universal (And secure), Civic Designing, Medium.com, Printed From Internet January 2019, 9 pgs.	
	2	Unisyn Voting Solutions, OpenElect FreedomVote Tablet (FVT), The Freedom To Adapt; 2017, 2 pgs.	
	3	Election Systems & Software, ExpressVote XL, Full face Universal Voting System, 2016, 2 pgs.	
	4	Election Systems & Software, ExpressVote, Universal Voting System As A Marker, 2016, 2 pgs.	
	5	United States Patent Application No. 16/560,222 filed 9/4/2019, titled "Optical Character Recognition Of Voter Selections For Cast Vote Records," 22 pages.	

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE	
Examiner Signature	Date Considered

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16745621
Filing Date	2020-01-17
First Named Inventor	JAMES M. CANTER
Art Unit	
Examiner Name	
Attorney Docket Number	HART:032C2

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Richard D. Egan/	Date (YYYY-MM-DD)	2020-01-28
Name/Print	Richard D. Egan	Registration Number	36788

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	38415643
Application Number:	16745621
International Application Number:	
Confirmation Number:	6960
Title of Invention:	Optical Character Recognition Of Voter Selections For Cast Vote Records
First Named Inventor/Applicant Name:	James M. Canter
Customer Number:	36275
Filer:	Richard D. Egan/Ellen Tucker
Filer Authorized By:	Richard D. Egan
Attorney Docket Number:	HART:032C2
Receipt Date:	28-JAN-2020
Filing Date:	
Time Stamp:	10:55:54
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	IDS_1.pdf	1036044	no	5
			5e6006d1223b93723b2c633b5b31fc5de02910a8		

Warnings:

Information:					
2	Foreign Reference	B1.pdf	1139856	no	26
			635ed45bae88202ada29fabbb68b99a54fa1d107e		
Warnings:					
Information:					
3	Non Patent Literature	C1.pdf	411397	no	9
			e16c512a9d8df5325642532257b83ec36d9e400e		
Warnings:					
Information:					
4	Non Patent Literature	C2.pdf	1646347	no	2
			a34ef45ce5aa4643769c638a1976a63f1e8bb6f5f		
Warnings:					
Information:					
5	Non Patent Literature	C3.pdf	1223949	no	2
			d9f7713d252ab5df5a9bf6c077f0f4934b51de6e		
Warnings:					
Information:					
6	Non Patent Literature	C4.pdf	1206463	no	2
			70455a999bc99e30fa4acc668df34f6cde67e978		
Warnings:					
Information:					
7	Non Patent Literature	C5.pdf	1334917	no	22
			49c7a3b9f1a96548f896080618bb93db2125da76		
Warnings:					
Information:					
Total Files Size (in bytes):			7998973		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA/82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	UNKNOWN
Filing Date	HEREWITH
First Named Inventor	JAMES M. CANTER ET AL.
Title	OPTICAL CHARACTER RECOGNITION OF VOTER SELECTIONS FOR CAST VOTE RECORDS
Art Unit	UNKNOWN
Examiner Name	UNKNOWN
Attorney Docket Number	HART:032C2

SIGNATURE of Applicant or Patent Practitioner

Signature	/Richard D. Egan/	Date (Optional)	
Name	Richard D. Egan	Registration Number	36788
Title (if Applicant is a juristic entity)			
Applicant Name (if Applicant is a juristic entity)			
NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.			
☐	*Total of _____ forms are submitted.		

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

Application Number	Filing Date

(Note: The boxes above may be left blank if information is provided on form PTO/AIA/82A.)

☒ I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above:

36275

OR

☐ I hereby appoint Practitioner(s) named in the attached list (form PTO/AIA/82C) as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the patent application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above. (Note: Complete form PTO/AIA/82C.)

Please recognize or change the correspondence address for the application identified in the attached transmittal letter or the boxes above to:

☐ The address associated with the above-mentioned Customer Number

OR

☒ The address associated with Customer Number: 36275

OR

Firm or Individual Name			
Address			
City	State	Zip	
Country			
Telephone	Email		

I am the Applicant (if the Applicant is a juristic entity, list the Applicant name in the box):

Hart InterCivic, Inc.

- ☐ Inventor or Joint Inventor (title not required below)
- ☐ Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)
- ☒ Assignee or Person to Whom the Inventor is Under an Obligation to Assign (provide signer's title if applicant is a juristic entity)
- ☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

SIGNATURE of Applicant for Patent

The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity).

Signature		Date (Optional)	4/5/13
Name	James Carter		
Title	Vice President of Engineering		

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ Total of forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	HART:032C2
		Application Number	
Title of Invention	Optical Character Recognition Of Voter Selections For Cast Vote Records		
<p>The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.</p> <p>This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.</p>			

Secrecy Order 37 CFR 5.2:

☐	Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)
--------------------------	---

Inventor Information:

Inventor	1				Remove	
Legal Name						
Prefix	Given Name	Middle Name	Family Name	Suffix		
	James	M.	Canter			
Residence Information (Select One) ☒ US Residency ☐ Non US Residency ☐ Active US Military Service						
City	Austin	State/Province	TX	Country of Residence	US	

Mailing Address of Inventor:

Address 1	10603 Winchelsea Drive					
Address 2						
City	Austin	State/Province	TX			
Postal Code	78750	Country	US			

Inventor	2				Remove	
Legal Name						
Prefix	Given Name	Middle Name	Family Name	Suffix		
	Drew	E.	Tinney			
Residence Information (Select One) ☒ US Residency ☐ Non US Residency ☐ Active US Military Service						
City	Austin	State/Province	TX	Country of Residence	US	

Mailing Address of Inventor:

Address 1	1501 Arcadia Avenue					
Address 2						
City	Austin	State/Province	TX			
Postal Code	78757	Country	US			

Inventor	3				Remove	
Legal Name						
Prefix	Given Name	Middle Name	Family Name	Suffix		
	Ievgen		Konovalenko			
Residence Information (Select One) ☒ US Residency ☐ Non US Residency ☐ Active US Military Service						

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	HART:032C2
		Application Number	
Title of Invention	Optical Character Recognition Of Voter Selections For Cast Vote Records		

City	Austin	State/Province	TX	Country of Residence	US
------	--------	----------------	----	----------------------	----

Mailing Address of Inventor:

Address 1	14302 Terisu Lane				
Address 2					
City	Austin	State/Province	TX		
Postal Code	78728	Country	US		
All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the Add button.					

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below. For further information see 37 CFR 1.33(a).			
☐ An Address is being provided for the correspondence information of this application.			
Customer Number	36275		
Email Address		Add Email	Remove Email

Application Information:

Title of the Invention	Optical Character Recognition Of Voter Selections For Cast Vote Records		
Attorney Docket Number	HART:032C2	Small Entity Status Claimed	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	4	Suggested Figure for Publication (if any)	4

Filing By Reference:

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)
☐ Request Not to Publish. I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application has not and will not be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	HART:032C2
		Application Number	
Title of Invention	Optical Character Recognition Of Voter Selections For Cast Vote Records		

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32). Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	☒ Customer Number	☐ US Patent Practitioner	☐ Limited Recognition (37 CFR 11.9)
Customer Number	36275		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, 365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78. When referring to the current application, please leave the "Application Number" field blank.

Prior Application Status	Pending				Remove
Application Number	Continuity Type		Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)	
	Continuation of		16560222	2019-09-04	
Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
16560222	Continuation of	16239607	2019-01-04	10445966	2019-10-15
Prior Application Status	Expired				Remove
Application Number	Continuity Type		Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)	
16239607	Claims benefit of provisional		62711212	2018-07-27	
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the Add button.					Add

Foreign Priority Information:

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	HART:032C2
		Application Number	
Title of Invention	Optical Character Recognition Of Voter Selections For Cast Vote Records		

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)ⁱ the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Application Number	Country ⁱ	Filing Date (YYYY-MM-DD)	Access Code ⁱ (if applicable)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button.

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

<p>☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.</p> <p>NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.</p>
--

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	HART:032C2
		Application Number	
Title of Invention	Optical Character Recognition Of Voter Selections For Cast Vote Records		

Authorization or Opt-Out of Authorization to Permit Access:

When this Application Data Sheet is properly signed and filed with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) - Unless box A in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO - Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

☐ A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

☐ B. Applicant **DOES NOT** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	HART:032C2
		Application Number	
Title of Invention	Optical Character Recognition Of Voter Selections For Cast Vote Records		

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant	1	<input type="button" value="Remove"/>
<p>If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.</p> <p style="text-align: right;"><input type="button" value="Clear"/></p>		
☒ Assignee	Legal Representative under 35 U.S.C. 117	Joint Inventor
Person to whom the inventor is obligated to assign.		Person who shows sufficient proprietary interest
If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:		
<div style="border: 1px solid black; height: 20px; width: 100%;"></div>		
Name of the Deceased or Legally Incapacitated Inventor: <div style="border: 1px solid black; height: 20px; width: 100%;"></div>		
If the Applicant is an Organization check here. ☒		
Organization Name	Hart InterCivic, Inc.	
Mailing Address Information For Applicant:		
Address 1	15550 Wells Port Drive	
Address 2		
City	Austin	State/Province TX
Country	US	Postal Code 78728
Phone Number		Fax Number
Email Address		
Additional Applicant Data may be generated within this form by selecting the Add button. <input type="button" value="Add"/>		

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	HART:032C2
		Application Number	
Title of Invention	Optical Character Recognition Of Voter Selections For Cast Vote Records		

Assignee 1				
Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.				
<input type="button" value="Remove"/>				
If the Assignee or Non-Applicant Assignee is an Organization check here. ☐				
Prefix	Given Name	Middle Name	Family Name	Suffix
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Mailing Address Information For Assignee including Non-Applicant Assignee:				
Address 1		<input type="text"/>		
Address 2		<input type="text"/>		
City	<input type="text"/>	State/Province	<input type="text"/>	
Country ⁱ	<input type="text"/>	Postal Code	<input type="text"/>	
Phone Number	<input type="text"/>	Fax Number	<input type="text"/>	
Email Address	<input type="text"/>			
Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. <input type="button" value="Add"/>				

Signature:

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). However, if this Application Data Sheet is submitted with the **INITIAL** filing of the application and either box A or B is not checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	/Richard D. Egan/		Date (YYYY-MM-DD)	2020-01-17
First Name	Richard D.	Last Name	Egan	Registration Number
				36788
Additional Signature may be generated within this form by selecting the Add button. <input type="button" value="Add"/>				

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	HART:032C2
		Application Number	
Title of Invention	Optical Character Recognition Of Voter Selections For Cast Vote Records		

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

**DECLARATION (37 CFR 1.63) FOR UTILITY APPLICATION
USING APPLICATION DATA SHEET (37 CFR 1.76)**

Title of Invention:

**OPTICAL CHARACTER RECOGNITION OF VOTER SELECTIONS FOR CAST
VOTE RECORDS**

As the below named inventor, I hereby declare that:

- This Declaration is directed to:

☒ The attached application, or
☐ United States application or PCT international application number
filed on

- The above-identified application was made or authorized to be made by me.
- I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.
- I further declare that I have reviewed and understand the contents of the above-identified application, including the claims.
- I acknowledge my duty to disclose to the United States Patent and Trademark Office (hereinafter "the Office") all information known to me to be material to patentability of the subject-matter which is claimed as defined in 37 C.F.R. §1.56.

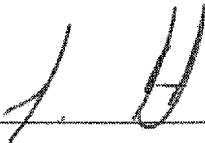
I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

LEGAL NAME OF INVENTOR

Inventor: James M. Canter

Date: 1/3/2019

Signature



**DECLARATION (37 CFR 1.63) FOR UTILITY APPLICATION
USING APPLICATION DATA SHEET (37 CFR 1.76)**

Title of Invention:

**OPTICAL CHARACTER RECOGNITION OF VOTER SELECTIONS FOR CAST
VOTE RECORDS**

As the below named inventor, I hereby declare that:

- This Declaration is directed to:

☒ The attached application, or
☐ United States application or PCT international application number
filed on

- The above-identified application was made or authorized to be made by me.
- I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.
- I further declare that I have reviewed and understand the contents of the above-identified application, including the claims.
- I acknowledge my duty to disclose to the United States Patent and Trademark Office (hereinafter "the Office") all information known to me to be material to patentability of the subject-matter which is claimed as defined in 37 C.F.R. §1.56.

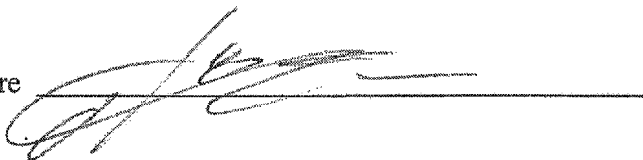
I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

LEGAL NAME OF INVENTOR

Inventor: Ievgen Konovalenko

Date: 11/3/2019

Signature



**DECLARATION (37 CFR 1.63) FOR UTILITY APPLICATION
USING APPLICATION DATA SHEET (37 CFR 1.76)**

Title of Invention:

**OPTICAL CHARACTER RECOGNITION OF VOTER SELECTIONS FOR CAST
VOTE RECORDS**

As the below named inventor, I hereby declare that:

- This Declaration is directed to:

☒ The attached application, or
☐ United States application or PCT international application number
filed on

- The above-identified application was made or authorized to be made by me.
- I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.
- I further declare that I have reviewed and understand the contents of the above-identified application, including the claims.
- I acknowledge my duty to disclose to the United States Patent and Trademark Office (hereinafter "the Office") all information known to me to be material to patentability of the subject-matter which is claimed as defined in 37 C.F.R. §1.56.

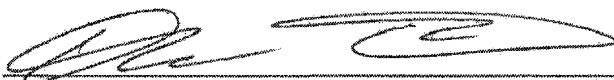
I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

LEGAL NAME OF INVENTOR

Inventor: Drew E. Tinney

Date: 11/3/2019

Signature



ABSTRACT

An electronic voting system is described that utilizes printed vote records (PVRs) in which a voter's vote selections are recorded in voter readable characters. Optical character recognition (OCR) techniques may then be utilized to scan the PVR to record the voter's selections. The OCR data is then utilized to generate the cast vote record. Thus, the electronic voting system directly interprets the voter selections from the PVR just as the voter sees the data. In this manner "what you see is what you get" printed vote record data is provided for a voter's viewing and that same data is used to generate the cast vote record.

What is claimed is:

1. A method for electronic voting using printed vote records, comprising:

generating a printed vote record of at least one vote selection of a voter;

providing, on the printed vote record, voter readable text indicating the voter's at least one vote selection;

providing, on the printed vote record, encoded data, the encoded data indicating the voter's at least one vote selection;

electronically scanning the voter readable text on the printed vote record to create a first data set, the first data set indicating the voter's at least one vote selection;

electronically scanning the encoded data on the printed vote record to create a second data set, the second data set indicating at least the voter's at least one vote selection;

comparing the first data set and the second data set; and

providing a cast vote record indicating the voter's at least one vote selection, an accuracy of the cast vote record confirmed based at least in part on a comparison of the voter's at least one vote selection as indicated by the first data set and the voter's at least one vote selection as indicated by the second data set.

2. The method of claim 1, wherein the encoded data includes at least one bar code.

3. The method of claim 2, wherein the bar code is a one dimensional bar code.

4. The method of claim 1, wherein the bar code is a two dimensional bar code.
5. The method of claim 4, wherein the two dimensional bar code is a QR code bar code.
6. The method of claim 1, utilizing the first data set and the second data set to confirm an integrity of the printed vote record.
7. The method of claim 6, wherein the integrity of the printed vote record is confirmed by comparing the first data set to information provided in the encoded data.
8. The method of claim 7, wherein the integrity of the printed vote record is confirmed by comparing a first hash produced from the first data set to a second hash provided in the encoded data.
9. The method of claim 6, further comprising comparing the first data set to an election dictionary, the election dictionary containing at least potential vote choices.
10. The method of claim 9, wherein the comparing the first data set to an election dictionary is utilized to confirm the accuracy of an optical character recognition (OCR) process.

11. The method of claim 1, further comprising comparing the first data set to an election dictionary, the election dictionary containing at least potential vote choices.

12. The method of claim 11, wherein the comparing the data set to an election dictionary is utilized to confirm the accuracy of to confirm the accuracy of an optical character recognition (OCR) process.

13. The method of claim 12, wherein the election dictionary contains at least one candidate name.

14. The method of claim 1, wherein the encoded data includes at least one bar code, bar code data of the bar code including data which is used to map the bar code to at least one particular vote selection.

15. The method of claim 14, wherein the vote choice is a particular candidate.

16. The method of claim 14, wherein the data which is used to map the bar code to at least one particular vote choice is hash data.

17. The method of claim 14, wherein the bar code data of bar code maps to the at least one particular vote selection through the use of a hash.

18. The method of claim 1, wherein the comparison of the first data set and the second data set is used to confirm that the at least one vote selection indicated by the first data set matches the at least one vote selection indicated by the second data set.

19. The method of claim 1, further comprising utilizing an election dictionary as part of the process to provide a cast vote record.

20. The method of claim 19, wherein the election dictionary includes at least a candidate name and other data affiliated with candidate name.

21. The method of claim 20, wherein the other data affiliated with a candidate name is a number.

22. The method of claim 21, wherein the number is a candidate sequence number or number indicative of a line of the printed vote record.

Patent Application for

Optical Character Recognition of Voter Selections for Cast Vote Records

Inventors: James M. Canter, Drew E. Tinney, Ievgen Konovalenko

BACKGROUND OF THE INVENTION

[0001] This application claims priority to Patent Application No. 16/560,222 filed September 4, 2019 which claims priority to Patent Application No. 16/239,607 filed January 4, 2019, now Patent No. 10,445,966, which claims priority to Provisional Patent Application No. 62/711,212 filed July 27, 2018, the disclosure of which is expressly incorporated herein by reference.

[0002] The present disclosure relates to the voting systems for elections. More specifically, it provides a system and method for providing paper records of voter selections and generating cast vote records from those paper records.

[0003] A variety of electronic voting systems are well known. Electronic systems include, for example, direct recording electronic (DRE) voting systems that electronically record votes to directly create an electronic cast vote record. Electronic systems also include, for example, systems in which paper vote records are generated based on a voter's electronic vote selections, with the paper vote record then being scanned for creation of the electronic cast vote record and electronic tabulation. As used herein, an electronic cast vote record is an electronic record that indicates the determined voter's choice or selection in a manner determined in accordance with the voting system. Thus, an electronic cast vote record is an electronic record of a voter's cast voting selections and may be used in the vote tabulation process.

[0004] The use of paper records in an electronic voting allows the creation of a paper trail of voter selections, for example for use by an elections office for audit purposes.

Such voting systems have also been called “hybrid voting” as it is a cross between all electronic DRE voting and paper-based hand-marked ballots. Such hybrid systems provide an electronic voting system in which a printed vote record (PVR) is produced (allowing a paper record to be an official record), and then the PVR is scanned on a digital scanner for cast vote record creation. The PVR may be full sized sheets of paper (for example standard 8.5 x 11 inch or 8.25 x 14 inch paper stock) or may be other specialized sizes. Traditionally, the PVR contains a barcode that is encoded with the voter’s vote selections. The barcode is then scanned with a scanner and decoded to generate the electronic cast vote record. It has been found though, that some voters may find such a process to lack transparency as the voter cannot readily review the barcode to confirm the encoded data matches the voter’s vote selections.

[0005] It would be desirable to provide an electronic voting system that utilizes PVRs in a manner that provides better transparency to the voter.

SUMMARY OF THE INVENTION

[0006] In one embodiment, the present disclosure describes an electronic voting system that utilizes printed vote records (PVRs) in which a voter’s vote selections are recorded in voter readable characters. Optical character recognition (OCR) techniques may then be utilized to scan the PVR to record the voter’s selections. The OCR data is then utilized to generate the cast vote record. Thus, the electronic voting system directly interprets the voter selections from the PVR just as the voter sees the data. In this manner “what you see is what you get” printed vote record data is provided for a voter’s viewing and that same data is used to generate the cast vote record.

[0007] Further, the OCR process utilized accounts for and corrects for potential OCR errors. In one embodiment, an election dictionary is provided of the potential vote choices. Thus, for example, candidate names may be entered into the election dictionary and utilized for pattern matching to the OCR results. To further ensure accuracy (and address candidates which may have the same or similar names), the

sequence number affiliated with a particular candidate may be utilized. Further, the line number (or even the contest title itself) on the PVR may also be utilized as a contest identifier. In one embodiment, the OCR'ed name and additional data may be utilized together as the key into the election dictionary. The additional data may be data related to a candidate, but being more than just the candidate name. For example, in some embodiments, the additional data may be the sequence number and/or line number data. Thus, for example, the OCR'ed name and sequence number, the OCR'ed name and line number, or the OCR'ed name, sequence number and line number may be utilized together as the key into the election dictionary. In addition, a long string matching algorithm may be utilized to provide error detection to the string. In one embodiment, the Levenshtein distance algorithm may be utilized for such string error detection. More specifically, the Levenshtein technique is used for error detection and the calculation of a "distance" between the OCR data and each key in the dictionary. If a calculated distance is below a defined threshold, then the data is matched to that dictionary entry. Then as described below, a hash check indicates if all of the matches were correct. In this manner, OCR data errors may be eliminated leading to a more robust OCR result which may be used for the subsequent generation of a cast vote record.

[0008] Further, to ensure the PVR is valid and/or has not been altered after printing, a barcode is also provided on the PVR. The barcode includes a single digitally signed hash that may be generated by using a secure hash function to indicate the PVR is valid and a one way hash of the voter's vote selections. As part of the scanning process, the optical character recognition results may be generated and then verified by use of another hash process. More specifically, a hash produced from the OCR generated characters may be compared to the hash provided in the barcode. Such techniques confirm that the PVR was printed from a known source and that the PVR has not been altered from its original state. In this manner, a counterfeit PVR or a PVR that has had its characters altered may be detected. Moreover, if the PVR was improperly or tampered with when printed this technique may detect such tampering.

[0009] To further ensure the accuracy of the OCR process, additional processing beyond traditional OCR processes may also be utilized for recognizing the characters presented on the PVR.

[0010] In one embodiment, a method for electronic voting using printed vote records is provided. The method comprises recording a voter's vote selections and generating a printed vote record of the voter's vote selections, the printed vote record containing voter readable text indicating the voter's vote selections. The method further comprises scanning the printed vote record, the scanning including scanning the voter readable text. The method also includes utilizing optical character recognition (OCR) on the scanned voter readable text to create a data set which identifies the voter's vote selections and generating a cast vote record from the data set so that voter selections in the cast vote record are based on the voter readable text.

[0011] In another embodiment, a method for electronic voting using printed vote records is provided. The method may comprise recording a voter's vote selection with a ballot marking device and generating a printed vote record of the voter's vote selections, the printed vote record containing voter readable text including a candidate name of a voter's vote selection. The method further comprises electronically scanning the printed vote record, the scanning including scanning the candidate name. The method also includes utilizing optical character recognition (OCR) on the scanned candidate name to create a first data set. The method further comprises comparing the first data set with an election dictionary and generating a cast vote record based on the comparing of the first data set with the election dictionary so that voter selections in the cast vote record are based on is based at least in part on the scanned candidate name.

[0012] In yet another embodiment, a method for electronic voting using printed vote records is provided. The method comprises recording a voter's vote selections and generating a printed vote record of the voter's vote selections, the printed vote record containing voter readable text indicating the voter's vote selections, the printed vote record further including a bar code. The method further comprises electronically scanning the printed vote record, the electronic scanning including scanning the voter readable text and scanning the bar code. The method also includes utilizing optical

character recognition (OCR) on the scanned voter readable text to create a data set which identifies the voter's vote selections and generating a cast vote record from the data set so that voter selections in the cast vote record are based on the voter readable text.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] A more complete understanding of the present invention and advantages thereof may be acquired by referring to the following description taken in conjunction with the accompanying drawings, in which like reference numbers indicate like features. It is to be noted, however, that the accompanying drawings illustrate only exemplary embodiments of the disclosed concept and are therefore not to be considered limiting of its scope, for the disclosed concept may admit to other equally effective embodiments.

[0014] Figure 1 illustrates an exemplary voting system for utilizing the techniques described herein.

[0015] Figure 2 illustrates an exemplary ballot marking device for utilizing the techniques described herein.

[0016] Figure 3 illustrates an exemplary printed vote record generated by the ballot marking device.

[0017] Figure 4 illustrates an exemplary printed vote record process flow utilizing the techniques described herein.

[0018] Figure 5 illustrates an exemplary process flow for matching OCR data to ballot choices.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0019] Figure 1 illustrates one exemplary embodiment of a voting system for utilizing the techniques described herein. It will be recognized, however, that the techniques

described herein may be utilized in a wide range of other voting systems. As shown in Figure 1, a voting system 10 that may be located at a polling location includes a ballot marking device (BMD) 15, a scanner 20 and a computing device 25. In one embodiment of a voting process, a polling official and/or the voter may activate a voting session on the BMD 15 (in one example by providing an access code to a voter to access the BMD 15). After activation, the voter may then make voting selections on the BMD 15. When the voter has completed their selections, the BMD 15 may then print out a PVR of the voter's voting selections. As described above and explained in more detail below, the voter's selections may be indicated on the PVR using readable characters so that the voter may visually confirm their voting selections, thus providing voting transparency to the voter. The voter may then enter the PVR into a scanner 20 which provides a scanned image of the PVR. The scanner 20 may provide that scanned image of the PVR to a computing device 25 which is connected to the scanner 25. The computing device may then perform an OCR process on the scanned image. The computing device 25 may also provide improved accuracy and/or error correction of the OCR by utilizing data processing techniques that are described herein to enhance the conversion of the scanned image to usable data. The scanning hardware for the scanner 20 may be conventional scanning hardware. However, as described in more detail below, specialized data analysis of the scanned information may be provided to improve the integrity and reliability of the scan. Such data analysis may be accomplished with the computing device 25. The computing device may then generate an electronic cast vote record associated with the voter's selections. It will be recognized that the functionality of the computing device may alternatively be integrated within the scanner 20. The BMD 15, scanner 20 and computing device 25 may each be separate non-integrated devices. Alternatively, all or some of the functionality of these devices may be integrated together within one device.

[0020] Figure 2 illustrates an exemplary BMD. However, it will be recognized that a wide range of other BMDs may be utilized while still achieving the advantages of the voting process described herein. The BMD 100 of Figure 2 includes a display 105, a voting processing unit 110 and a printer medium input tray 115. The voting processing unit 110 may include a variety of hardware and software, including a memory, processors,

associated election software, input devices, etc., all as is known in the art. In operation, a voter may utilize the BMD 100 as part of the process of casting a vote in an election. The voter may be provided instructions and voting choices that are presented on the display 105 of the BMD 100. Various voter responses and election selections may be entered via the display (in the case of a touchscreen display) or may entered via other inputs such as a keypad, buttons, dials, etc. that may be part of the voting processing unit 110. The BMD 100 also includes an internal printer (not shown). The printer may be utilized to print a voter's selections on a PVR. In one embodiment, the printer may be a thermal printer and the PVR may be printed on thermal paper. In operation, a voter uses the BMD 100 to generate a PVR. The PVR may then be scanned and processed as described elsewhere herein to create an electronic cast vote record. As described herein, the PVR may be utilized not only as part of the cast vote record generation process, but also as a tool for the voter to inspect the generated vote selections prior to casting the voter selections through the scanning process.

[0021] As described herein, the BMD may be a hybrid voting device that combines electronic voting features with the production of a PVR. Such a technique allows voting transparency to the voter and provides the election officials a paper record which may be used for audit or other purposes. The PVR may be a full sheet of standard paper stock or may be other customized sizes. As described herein, OCR may be used to determine the voter selections with the add-on of additional data process techniques to ensure data accuracy of the OCR process and ensure validity of the PVR.

[0022] As mentioned, OCR techniques may be utilized to scan the PVR to record the voter's selections. The OCR data is then utilized to generate the cast vote record. Thus, the electronic voting system directly interprets the voter selections from the PVR just as the voter sees the data. In this manner "what you see is what you get" printed vote record data is provided for a voter's viewing and that same data is used to generate the cast vote record.

[0023] Further, the OCR process utilized accounts for and corrects for potential OCR errors. In one embodiment, an election dictionary is provided of the potential vote choices. Thus, for example, candidate names may be entered into the election

dictionary and utilized for pattern matching to the OCR results. To further, ensure accuracy (and address candidates that have the same or similar names) additional information beyond just the candidate name be utilized for comparison to the election dictionary. Thus, in one embodiment, the OCR'ed name and additional data may be utilized together as the key into the election dictionary. The additional data may be data related to a candidate, but being more than just the candidate name. For example, in some embodiments, the additional data may be the sequence number data affiliated with a candidate. The additional data may also be line number data affiliated with a contest, and/or the contest name itself. Thus, for example, the OCR'ed name and sequence number, the OCR'ed name and line number, or the OCR'ed name, sequence number and line number may be utilized together as the key into the election dictionary. It will be recognized that other combinations of a candidate name and additional data may also be used.

[0024] In addition a long string matching algorithm may be utilized to provide error detection to the string. In one embodiment, the Levenshtein distance algorithm may be utilized for such string error detection. More specifically, the Levenshtein algorithm is used for error detection and the calculation of a “distance” between the OCR data and each key in the dictionary. If a calculated distance is below a defined threshold, then the data is matched to that dictionary entry. Then as described below, a hash check indicates if all of the matches were correct. In this manner, OCR data errors may be minimized and a more robust OCR result may be obtained and used for the subsequent generation of a cast vote record.

[0025] The scanned data for write-in candidates may be treated somewhat differently as the names of write-in candidates may not be available before the voting process for entry in an election dictionary to use in the OCR post-processing steps as described above. In one embodiment, write-in data may be saved in two parts as part of the cast vote record. First, a PNG snippet of the entered write-in data (a photo “snapshot”) may be stored as part of the cast vote record. Second, the OCR digital results of the write-in data are also stored. Both parts may then be included in the cast vote record and uploaded for tabulation. When the election office processes write-in votes, the election office will have the digital OCR data side by side with the write-in image so that manual

adjudication (if desired) may be accomplished. In one embodiment, further additional back office write-in candidate data verification may be accomplished if the election office generates a certified write-in candidate list. More particularly, the names from the certified write-in candidate list may be entered into the back office post-processing computer systems and then used in the same manner that the election dictionary described above is used to provide enhanced accuracy to the OCR results for write-in candidates.

[0026] Further, to ensure the PVR is valid and/or has not been altered after printing, a barcode is also provided on the PVR. The barcode includes a single digitally signed hash that may be generated using a secure hash function to indicate the PVR is valid and a one way hash of the voter's vote selections. As part of the scanning process, the optical character recognition results may be generated and then verified by use of another hash process. More specifically, a hash produced from the OCR generated characters may be compared to the hash provided in the barcode. Such techniques confirm that the PVR was printed from a known source and that the PVR has not been altered from its original state. In this manner, a counterfeit PVR or a PVR that has had its characters altered may be detected. Moreover, if the PVR was improperly or tampered with when printed, this technique can detect such tampering. It is noted that the barcode is used to confirm data accuracy and PVR integrity but, in one embodiment does not have to be used to determine voter selections. The barcode could be any of a wide range of barcode types, including for example, one dimensional barcodes or a matrix two-dimensional barcode (such as for example a QR code). Further, though described as one barcode, it will be recognized that the barcode may be split across multiple barcodes as well. For example, each barcode could serve as a landmark and the found barcode positions could be used to correct for scanning skew.

[0027] An exemplary PVR provided by the BMD 100 of Figure 2 is shown in Figure 3. As shown in Figure 3, a PVR 300 is provided. The PVR may include a header region 310 in which a variety of information may be printed. In one example, the header region 310 may include instructions to the voter, information regarding the election, a PVR number, page information, etc. As shown, in one embodiment a barcode 320 may be provided in the header region. In the example shown, the barcode is in the form of a QR code;

however, other barcodes may be utilized. As described above, the barcode may be used to confirm data accuracy and/or PVR integrity but, in the exemplary embodiment, is not used to determine voter selections. The election voting contests may be shown in the contest section 330 of the PVR 300 as shown. Further, the voter's selections may be shown in the voter selection section 340 of the PVR 300 as shown. As seen in Figure 3, the voter selections are provided in a character form that is readable by the voter. Thus, voting transparency is provided to the voter such that the voter can confirm the PVR matches the selections entered by the voter on the BMD 100.

[0028] The contents of the barcode 320 may contain a wide variety of information including metadata content and hash data content. In one exemplary embodiment, the metadata content may include, but is not limited to a PVR barcode version, an election ID number, other unique ID numbers, an election version, precinct split sequence number, party sequence number, a crossover ballot flag, provisional ballot flag, official versus test ballot flag, accessibility settings, sheet number, sequence number of the first contest on the sheet, the number of lines on the sheet, etc. One use of the hash content is to ensure all voter selections were read correctly. Another use of the hash content is to verify the validity of the PVR itself. The hash may cover, in one embodiment, ballot metadata sections and all printed data in the voter selection section 340.

[0029] Thus, the barcode uses a single digitally signed hash that can be used for multiple purposes. First, the single digitally signed hash may be used to ensure the source origin of the PVR (that it came from the BMD 100), since it is a digital signature. In addition, the one way hash of voter selections provided in the barcode can be used to for a comparison to a hash of the OCR voter selections. The comparison of the one way hash of the barcode to the hash of OCR results can confirm that the PVR was not edited after printing. For example, if a voter's selection was edited on the PVR after printing from a first candidate name to a second candidate name, the OCR process would decode the second candidate name, but when hash checked, the first candidate name would have been utilized to create the barcode hash, and thus the hash check would fail. In this manner, though the barcode contains a hash of the voter selection data, the barcode does not contain the original voter selection data itself.

[0030] Figure 4 illustrates one exemplary PVR processing workflow utilizing a PVR such as PVR 300 of Figure 3. It will be recognized that the workflow of Figure 4 is merely one exemplary workflow and many other workflows may utilize the techniques disclosed herein. As shown in the workflow of Figure 4, a scanned PVR is analyzed in accordance with the flow diagram of the workflow starting with a PVR scan and ending with either a rejected ballot or a cast or review of the ballot. As shown in Figure 4, the workflow starts with step 400 of starting a PVR scan. Next, at step 405 the barcode is decrypted and at step 405 it is determined if the decrypt succeeded. If the decryption was successful the workflow proceeds to step 415. If the decryption was not successful the workflow proceeds to step 420 where the workflow ends and the PVR is rejected. At step 515, the PVR is analyzed to determine if it is allowed. If the PVR is allowed the workflow proceeds to step 425 and if the PVR is not allowed, the workflow proceeds to step 420 where the workflow ends and the PVR is rejected. At step 425, the PVR is subjected to an OCR process. At step 430, the output of the OCR is analyzed to confirm it has a valid output (for example the correct number of lines, etc.). If no, the workflow proceeds to step 420 where the PVR is rejected. If yes, the workflow proceeds to step 435.

[0031] At step 435 the OCR data is matched to the ballot choices. Then at step 440 the hash is checked and if the hash matches at step 450 the workflow proceeds to step 460. If the hash does not match the process proceeds to step 455 where it is determined if there are still valid alternatives to try. If there are no valid alternatives to try, the workflow proceeds from step 455 to step 420 where the PVR is rejected. If there are valid alternatives to try at step 455, the workflow proceeds to step 440 it is determined if the number of contests with an alternate is under a threshold. If the answer is no at step 440, workflow to step 420 where the PVR is rejected. If the answer is yes at step 440, workflow proceeds to step 445 where alternates are swapped in. Workflow then proceeds again to step 440 and steps 440 and 450 are performed again as described above. At step 460, all write-in areas are snipped. From step 460, the process proceeds to step 465 to add OCR text to snippets and then the process ends at step 470 where the PVR is cast or reviewed.

[0032] It is noted that, as part of the workflow of Figure 4, a process step occurs that matches the OCR data to ballot choices, for example at step 435 of Figure 4. Details

regarding this process step are shown in more detail in Figure 5. It will be recognized that the workflow of Figure 5 is merely one exemplary matching workflow and many other workflows may utilize the techniques disclosed herein. As shown in Figure 5, a process is shown for ballot choice matching for each OCR entry. As shown in step 500, the workflow of Figure 5 begins with an OCR entry. At step 505, the workflow concatenates the choice name and additional data (in this example a sequence number) and the value for each possible ballot choice to create comparison strings. Note, this may include “no selection” strings to account for the situation where no selection is made by the voter. Then at step 510, the process finds the comparison string with the lowest Levenshtein distance to the OCR string. Next at step 515, it is determined if the Levenshtein distance is under a threshold. If yes, the process proceeds to step 525. If no, the process proceeds to step 520 and the printed vote record is rejected. At step 525 it is determined if any other choices have the same distance. If no, the process proceeds to step 535. If yes, the process proceeds to step 530. At step 535 the choice provided is used and the process proceeds as shown in Figure 4 and described above. At step 530, the other choices are added to the valid alternatives list and the process then proceeds to step 535.

[0033] Thus, as described herein, a PVR is provided that is readable by a voter. Further, the readable text is utilized to generate an electronic cast vote. By being readable, full voter verification of a voter’s vote selections is provided in a format that provides transparency to the voting process. An OCR process is performed on the PVR and the output of the OCR process is further processed in order to ensure data integrity and reliability. In one embodiment, an election dictionary is provided of the potential vote choices and the election dictionary and other data on the PVR is utilized to provide reliable matching of the OCR results with the proper ballot choice. A barcode and hash process may further be utilized to ensure PVR integrity and security. Thus, a voter’s choices are shown in text and OCR techniques are utilized while a barcode is utilized for PVR and choice verification. In this manner, a secure, reliable and transparent voting workflow is provided.

[0034] Further modifications and alternative embodiments of this invention will be apparent to those skilled in the art in view of this description. Accordingly, this

description is to be construed as illustrative only and is for the purpose of teaching those skilled in the art the manner of carrying out the invention. It is to be understood that the forms and methods of the invention herein shown and described are to be taken as presently preferred embodiments. Equivalent techniques may be substituted for those illustrated and described herein and certain features of the invention may be utilized independently of the use of other features, all as would be apparent to one skilled in the art after having the benefit of this description of the invention.

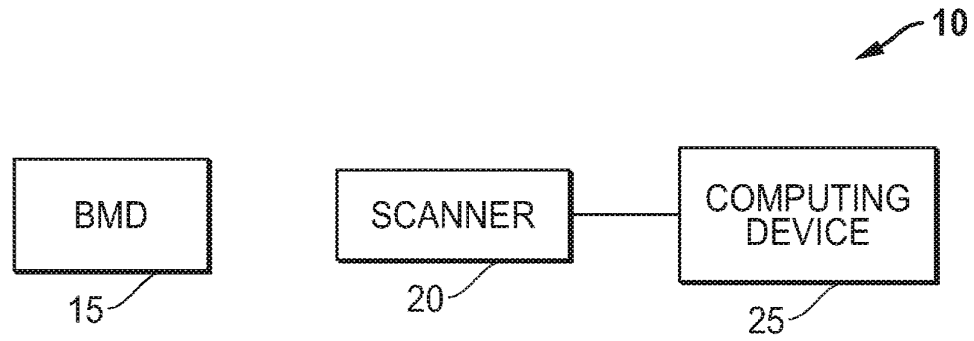


FIG. 1

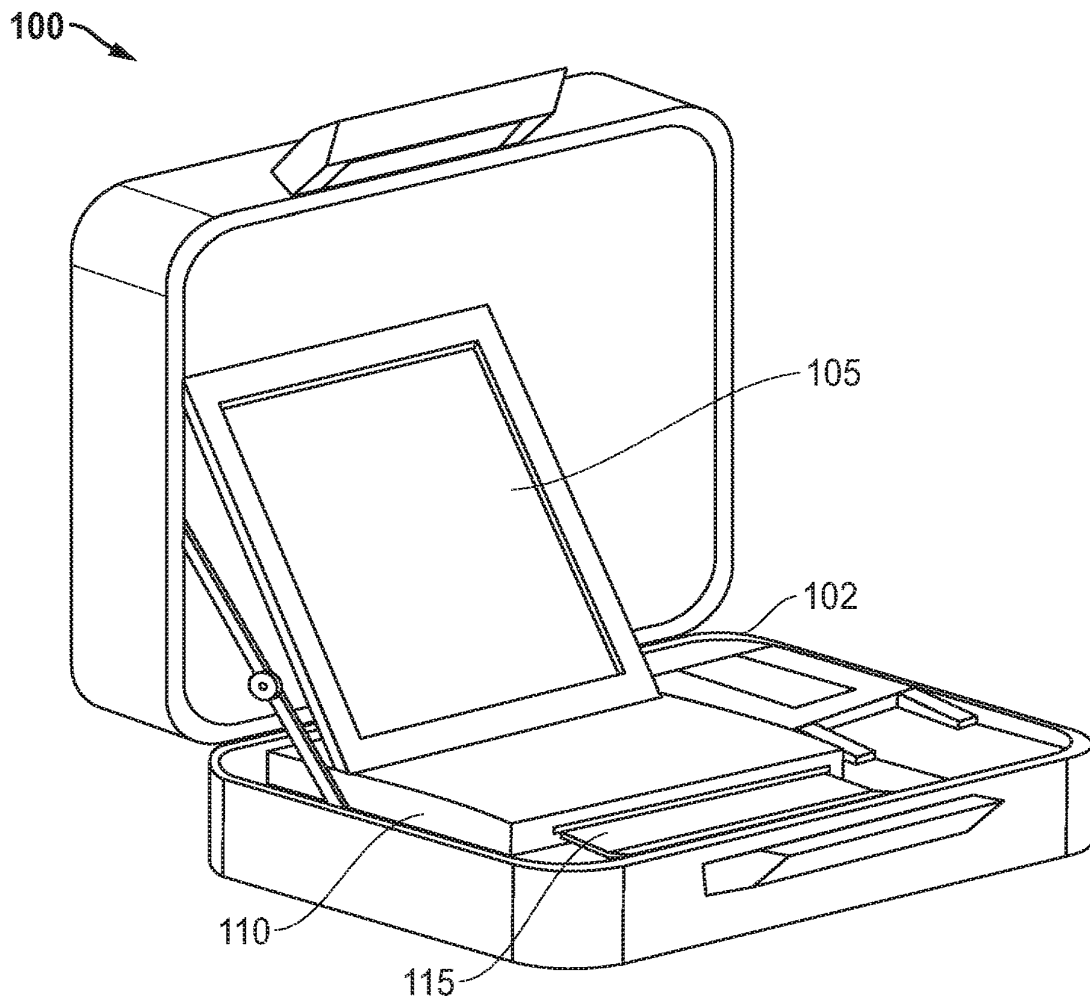


FIG. 2

320

300

310

340

OFFICIAL VOTE RECORD

Additional custom header text

PUR Title

Joint General and Special Election

Sample County, USA

November 7, 2006 91234567

Precinct: Anderson 1001-A

PROVISIONAL

044498-12-MBEV

23

BO: 8ja-svtd-mby4

Page 1 of 3

To cast your ballot, you must take this record to the separate scanning station and scan it.

	CHOICE	ORDER	
President and Vice President	QUINLAN PHILLIPS	3	DEM
Senator	CAJ KLEMENTS	1	DEM
House of Representative District 6	NITIN STEVENS	5	DEM
Secretary of State	VIMAL ORIOI	22	DEM
Railroad Commissioner	KELEMEN ANGIOLI	2	DEM
State Senator	SALLIE UTKIN	4	DEM
State Legislator, District 124	SEBASTIJAN KAMAU	6	DEM
Governor	TEKLA ALFARSI	1	DEM
State Judge, 15th District	LASERBEAK ANDREASSEN	3	DEM
District Judge, 3rd District	ALEID MARTIN	165	DEM
Appeals Court Judge	FEDOT OKONKWO	7	DEM
Sample County Sheriff	*NO SELECTION*		
Sample County Tax Commissioner	MOTKE DOWNER	1	DEM
Sample County Water Supervisor	MARTZEL DANIEL	8	W-I
Sample County Chief Librarian	KENANIAH ARMSTRONG	2	DEM
Community College Director	ABRIEL BENTON	1	DEM
Community College Board Member S. 1	DALTON BROOK	6	DEM
Mayor of Sample City	KOHAKU TESTA	9	DEM
City Oversight Board, Position 1	WAT JOKUMSEN	11	DEM
City Oversight Board, Position 2	TATE DOBOS	2	DEM
City Oversight Board, Position 3	KATIDA KLERX	4	DEM
City Oversight Board, Position 4	PHILE BAAS	12	DEM
City Oversight Board, Position 5	NAIARA CHAUDHRI	7	DEM
City Oversight Board, Position 6	LARKIN DONOHUE	1	DEM
City Oversight Board, Position 7	KAY PHILLIPS	3	DEM
City Oversight Board, Position 8	*NO SELECTION*		
Proposition 1	YES	1	
Proposition 2	NO	2	
Proposition 3	NO	2	
Proposition 4	YES	1	
School Board Member, Sample ISD	KUNTO MOSES	1	DEM
	2 (TWO) VOTES		
	ALDEGAR KRAEMER	5	DEM
	1 (ONE) VOTE		
	<SPACE>		
	<SPACE>		
Should TARA DOUGLASS be recalled?	NO	2	
Candidates to replace TARA DOUGLASS	<NOT APPLICABLE>		
City Council	DENNY ABIODUN	21	DEM
	RANK 1 (ONE)		
	CONWAY BRIOSCHI	4	DEM
	RANK 2 (TWO)		
	FLANAGAN BEULEN	13	DEM
	RANK 3 (THREE)		
	END OF PAGE		

FIG. 3

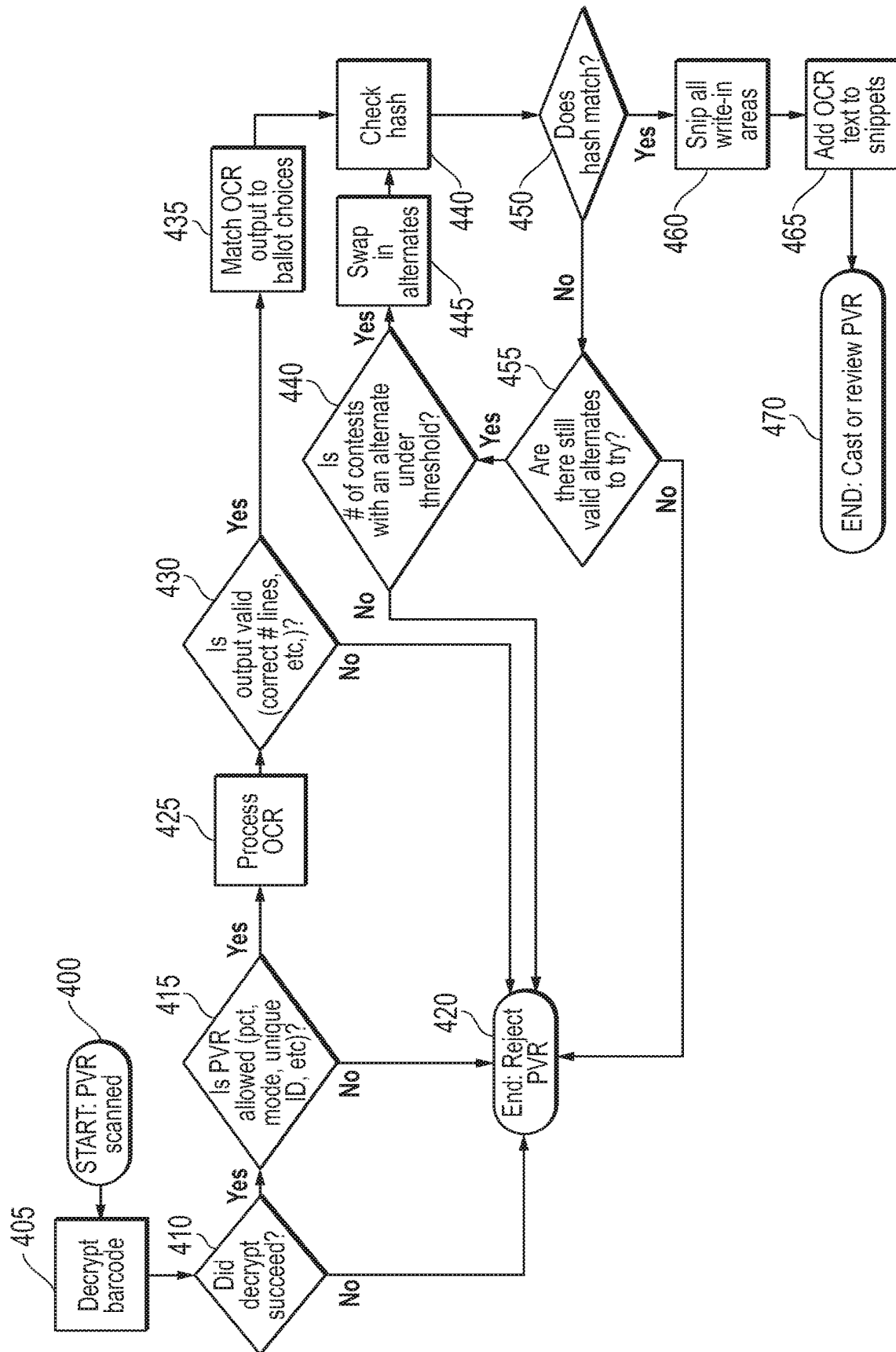


FIG. 4

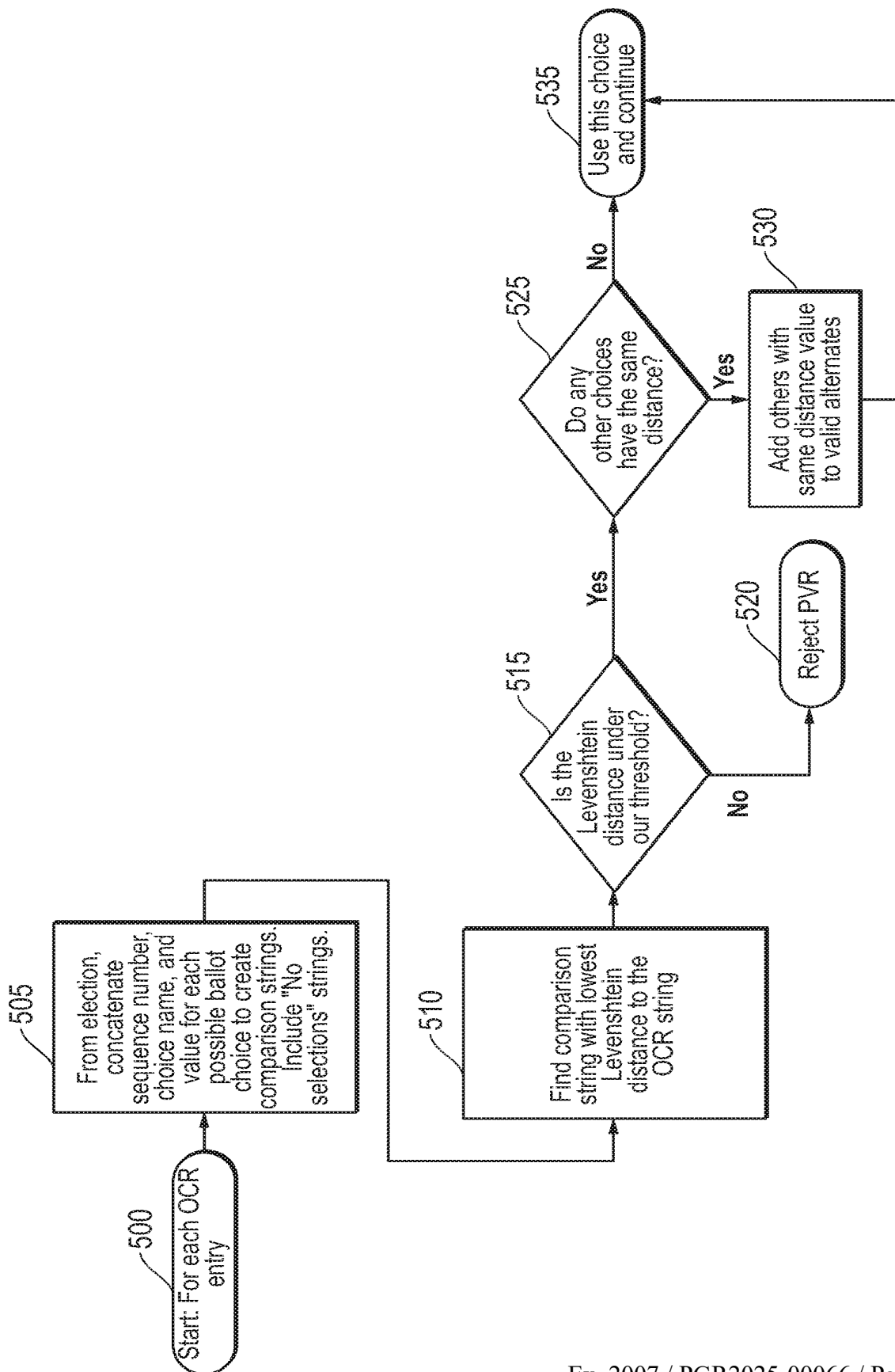


FIG. 5

Electronic Patent Application Fee Transmittal				
Application Number:				
Filing Date:				
Title of Invention:		OPTICAL CHARACTER RECOGNITION OF VOTER SELECTIONS FOR CAST VOTE RECORDS		
First Named Inventor/Applicant Name:		James M. Canter		
Filer:		Richard D. Egan/Marty Jones		
Attorney Docket Number:		HART:032C2		
Filed as Large Entity				
Filing Fees for Utility under 35 USC 111(a)				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
UTILITY APPLICATION FILING	1011	1	300	300
UTILITY SEARCH FEE	1111	1	660	660
UTILITY EXAMINATION FEE	1311	1	760	760
Pages:				
Claims:				
CLAIMS IN EXCESS OF 20	1202	2	100	200
Miscellaneous-Filing:				
Petition:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				1920

Electronic Acknowledgement Receipt

EFS ID:	38325854
Application Number:	16745621
International Application Number:	
Confirmation Number:	6960
Title of Invention:	OPTICAL CHARACTER RECOGNITION OF VOTER SELECTIONS FOR CAST VOTE RECORDS
First Named Inventor/Applicant Name:	James M. Canter
Customer Number:	36275
Filer:	Richard D. Egan/Marty Jones
Filer Authorized By:	Richard D. Egan
Attorney Docket Number:	HART:032C2
Receipt Date:	17-JAN-2020
Filing Date:	
Time Stamp:	11:50:42
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	\$ 1920
RAM confirmation Number	E20201GB51135664
Deposit Account	101205
Authorized User	Marty Jones

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

37 CFR 1.16 (National application filing, search, and examination fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

Ex. 2007 / PGR2025-00066 / Page 555 of 557

Election Systems & Software, LLC v. Hart Intercivic, Inc.

37 CFR 1.19 (Document supply fees)
 37 CFR 1.20 (Post Issuance fees)
 37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Power of Attorney	poa.pdf	226669	no	2
			a7c1875d0bb11b08f0e896950ec935c551e8cb6d		
Warnings:					
Information:					
2	Application Data Sheet	ADS.pdf	1823313	no	9
			c22de778d5f577f9989838f2f5ea908bdb1d286b		
Warnings:					
Information:					
3	Oath or Declaration filed	Decs.pdf	319811	no	3
			adb261580c49407ed1e855224c2d374fd0f8da6b		
Warnings:					
Information:					
4		Patentapp.pdf	90841	yes	18
			32698057213f62dc97c6370311b5b872a81ee610		
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Abstract		18	18	
	Claims		14	17	
	Specification		1	13	
Warnings:					
Information:					
5	Drawings-only black and white line drawings	Figures.pdf	309023	no	4
			6a1279ffb80938e13c464557206f6a9a818a		

Ex. 2007 / PGR2025-00066 / Page 556 of 557

Election Systems & Software LLC v. Hart Intercivic, Inc.

Warnings:					
Information:					
6	Fee Worksheet (SB06)	fee-info.pdf	36435	no	2
			9c8f7e1ef08d92785ebdfd8810e1440561b474c8		
Warnings:					
Information:					
Total Files Size (in bytes):			2806092		
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					