



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
62/267,393	12/15/2015		130	WHIT US-1PRV(040492.0002)		

27104
FENNEMORE CRAIG, P.C.
1700 Lincoln Street Suite 2400
DENVER, CO 80203

CONFIRMATION NO. 9782
FILING RECEIPT



Date Mailed: 02/08/2016

Receipt is acknowledged of this provisional patent application. It will not be examined for patentability and will become abandoned not later than twelve months after its filing date. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, 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 Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections 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**

Inventor(s)

Peter Whitmarsh, Las Vegas, NV;
Shana Whitmarsh, Las Vegas, NV;

Applicant(s)

Tradewinds Technology, LLC, Las Vegas, NV;

Power of Attorney:

Bruce Dahl--33670

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: 02/08/2016

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 62/267,393**

Projected Publication Date: None, application is not eligible for pre-grant publication

Non-Publication Request: No

Early Publication Request: No

**** SMALL ENTITY ****

Title

UAV DEFENSE SYSTEM

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 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.

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	WHIT US-1PRV(040492.0002)
		Application Number	
Title of Invention	UAV DEFENSE SYSTEM		
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. 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.			

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	
	Peter		Whitmarsh		
Residence Information (Select One) ☒ US Residency ☐ Non US Residency ☐ Active US Military Service					
City	Las Vegas	State/Province	NV	Country of Residence	US

Mailing Address of Inventor:

Address 1	300 S. Fourth Street, Suite 1400				
Address 2					
City	Las Vegas	State/Province	NV		
Postal Code	89101	Country	US		

Inventor	2				Remove
Legal Name					
Prefix	Given Name	Middle Name	Family Name	Suffix	
	Shana		Whitmarsh		
Residence Information (Select One) ☒ US Residency ☐ Non US Residency ☐ Active US Military Service					
City	Las Vegas	State/Province	NV	Country of Residence	US

Mailing Address of Inventor:

Address 1	300 S. Fourth Street, Suite 1400				
Address 2					
City	Las Vegas	State/Province	NV		
Postal Code	89101	Country	US		

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button.

Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	WHIT US-1PRV(040492.0002)
		Application Number	
Title of Invention	UAV DEFENSE SYSTEM		

☐ An Address is being provided for the correspondence information of this application.

Customer Number	27104		
Email Address	ip@fclaw.com	Add Email	Remove Email

Application Information:

Title of the Invention	UAV DEFENSE SYSTEM		
Attorney Docket Number	WHIT US-1PRV(040492.0002)	Small Entity Status Claimed	☒
Application Type	Provisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)		Suggested Figure for Publication (if any)	

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.

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	27104		

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	WHIT US-1PRV(040492.0002)
		Application Number	
Title of Invention	UAV DEFENSE SYSTEM		

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		Remove	
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the Add button.			Add

Foreign Priority Information:

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).

			Remove
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.			Add

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ 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. 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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number WHIT US-1PRV(040492.0002)	
	Application Number	
Title of Invention	UAV DEFENSE SYSTEM	

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	WHIT US-1PRV(040492.0002)
		Application Number	
Title of Invention	UAV DEFENSE SYSTEM		

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	Remove
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. Clear		
☒ 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:		
Name of the Deceased or Legally Incapacitated Inventor:		
If the Applicant is an Organization check here. ☒		
Organization Name	Tradewinds Technology, LLC	
Mailing Address Information For Applicant:		
Address 1	300 S. Fourth Street, Suite 1400	
Address 2		
City	Las Vegas	State/Province NV
Country	US	Postal Code 89101
Phone Number		Fax Number
Email Address		
Additional Applicant Data may be generated within this form by selecting the Add button. 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	WHIT US-1PRV(040492.0002)
		Application Number	
Title of Invention	UAV DEFENSE SYSTEM		

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.				
Remove				
If the Assignee or Non-Applicant Assignee is an Organization check here. ☐				
Prefix	Given Name	Middle Name	Family Name	Suffix
Mailing Address Information For Assignee including Non-Applicant Assignee:				
Address 1				
Address 2				
City		State/Province		
Country ⁱ		Postal Code		
Phone Number		Fax Number		
Email Address				
Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. Add				

Signature:[Remove](#)

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	/Bruce E. Dahl/		Date (YYYY-MM-DD)	2015-12-15
First Name	Bruce	Last Name	Dahl	Registration Number
				33670
Additional Signature may be generated within this form by selecting the Add button. Add				

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	WHIT US-1PRV(040492.0002)
		Application Number	
Title of Invention	UAV DEFENSE SYSTEM		

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.

UAV DEFENSE SYSTEM

Technical Field

[0001] The present invention relates to defense systems in general and more particularly to systems for defending against unauthorized incursions by unmanned aerial vehicles.

Background

[0002] Unmanned aerial systems (UAS), unmanned aerial vehicles (UAVs), or drones are well-known in the art and are used for a wide variety of purposes. Unfortunately, it is possible to weaponize UAVs or drones, which may then be flown into public areas undetected and non-defended. Drone use will become the terrorist's primary choice for weaponry. There is currently no true defense against this kind of weaponry and there is no reliable detection, since air traffic control systems and satellites presently cannot detect them and there are no other detection systems at this time that are sensitive or responsive enough to prevent individual threats or attempts at terrorism or mass-destruction.

Detailed Description of Preferred Embodiments

[0003] Various embodiments of a drone defense system (DDS) are shown and described herein as they could be used to effect one or more countermeasures against unwanted or unauthorized drone incursions into defined air space. Additional information regarding the present invention is contained in Attachment A, which is attached hereto and forms a part of the disclosure.

[0004] The drone defense system may be used in any of a wide range of applications and environments. For example, embodiments of the drone defense system may be used in fixed locations, such as military installations, prisons, post offices, banks, airports, hospitals, and other secure areas where control and/or protection

of immediate airspace is desired. Other embodiments may be configured for use on aircraft (commercial and passenger jets, helicopters, and military aircraft, including military drones), ships, submarines, and land vehicles. Other embodiments may be deployed for use on roads, highways, and train tracks. The drone defense system could also be used in conjunction with indoor and outdoor sports and entertainment venues, such as arenas, stadiums, and theaters, just to name a few.

[0005] Still other embodiments of the drone defense system may be configured for use on cargo/freight ships, cruise ships, yachts, aircraft, trucks, and trains. Embodiments of the drone defense system may also be configured for use in office buildings, high-rises, manufacturing plants, and agriculture. The drone defense system could also be used in residential applications, in which case it may be integrated or configured to operate with home security and alarm systems. In other embodiments, portions of the drone defense system could be adapted for use in conjunction with wearable devices, such as wristbands, watches, and clothing, and also could be used in cars, small aircraft, gliders, and the like operated by consumers and hobbyists.

[0006] The drone defense system is capable of countering, mitigating and/or interdicting of unmanned aerial systems and unmanned aerial vehicles. The drone defense system may also involve a remote transmission security system (RTSS) which may be used to take control of or commandeer an unauthorized, undesired, or rogue drone to the point of returning it back to the sender while capturing and recording its location and if the rogue drone is equipped with a camera, take a photo of the rogue drone operator's face or any other physical ID. The RTSS process can include other forms of response. One example is having an armed security drone automatically respond to the tagged drones that have trespassed in a secure area as an extra countermeasure, in addition to

documenting the location of origin where the rogue drone was launched. The DDS has several countermeasure behaviors that can be programmed into the Remote Transmission Security System, which allows for further customization.

[0007] The RTSS operates in conjunction with one or more 'smart' devices comprising the drone defense system, such as, for example, sonar/radar sensors and applications that work with other components, including highly specialized classified security firmware and classified security software. RTSS is the first defensive system that can ID a drone's signature. When all parts are connected and applied, a logic control response is activated to keep the property secure and safe.

[0008] The RTSS constantly analyzes all of the parameters of the network that it is monitoring and it continuously processes all information from different UAS or drone signatures that are hostile and non-hostile that come within a 10-mile, 5-mile, and 1-mile area of a defined airspace system that is to be protected. The RTSS is thus an important aspect of the drone defense system: The RTSS creates a virtual 'dome' to protect the defined airspace that is to be protected.

[0009] The primary function of the RTSS is to identify and detect unauthorized or hostile drones in and around the area or region that is to be protected. Imagine a virtual three-dimensional dome covering the facility with all zones mapped as coordinates and points within the drone defense system. The system creates a buffer between the protected facility and the unauthorized or hostile drone with specific countermeasures applied to each zone.

[0010] The first process for RTSS after detection is tracking and analyzing all signatures of the different devices, elements, and components within protected zones. RTSS determines threat level and identifies (IDs) the drones. In one embodiment, the RTSS

identifies, classifies, and categorizes the unauthorized or hostile drones by their signatures. Each movement is computed and observed. Each tracking signature may be processed in conjunction with one or more information databases, including, for example a local database or a national database (the national registry database structure is currently being defined) to record the signature of each non-recognized signature and each event. The RTSS will record them and once the national database is online, it will attempt to match the signature of the drone or device with its owner. The behavior of the unauthorized or hostile drone is recorded with its signature identification. If the tracking signature matches a rule in the logic system that the unauthorized or hostile drone's identification signatures are a threat, the RTSS 'tags' the drone as unauthorized or even as hostile. Immediately, a series of processes are started to determine what rule of engagement will be applied on the intruding drone. The engagement responses are determined by the behavior of the hostile drone and other instructions. If there is a threat, the system will take the next step to response. These actions occur in milliseconds from the feeds of the apparatus; there are constant communications with the internal (local) and national databases.

[0011] The response engagement will determine what type of countermeasure would occur and at what distance. Exemplary countermeasures that may be applied or executed by the drone defense system include, but are not limited to, the following countermeasures:

- 1) "Return to Sender." This countermeasure involves the capture of a photo or image of the operator or pilot of the hostile drone. Images of other incriminating evidence may also be captured or obtained. RTSS will document the signature and event of trespass, and capture control of the hostile drone in

order to return it to its sender while using the onboard camera on a camera-equipped drone.

- 2) Intercept Hostile (Rogue) Drone by Armed Security Drones. In this countermeasure the RTSS can notify separate armed drone systems that there is an intrusion in the protected area. The armed drones may then intercept (e.g., shoot down) the unauthorized or hostile drone.
- 3) Commandeer. In this countermeasure, the RTSS actually takes over control of the hostile or unauthorized drone, forcing it to land away from the protected area. Law enforcement agencies (e.g., local law enforcement, the FBI, the DHS, etc) may then be notified and appropriate action taken.
- 4) Drone Destruct. In this countermeasure, the RTSS also takes over control or commandeers the hostile or unauthorized drone and may cause it to self-destruct or otherwise become inoperable (e.g., by initiating a power overload in the drone's power supply system).

[0012] In some embodiments, the drone defense system is configured or programmed to consider all drones to be hostile if their ID is not recorded as friendly or sanctioned by protected facilities, or adverse classified behaviors from an ID signature drone that crosses a specific zone.

[0013] In some embodiments, a general operational environment and/or parameters for the drone defense system (DDS) may be as follows:

- 1) The DDS will be able to determine between friendly and hostile drones.
- 2) DDS coverage includes three-dimensional (e.g., X,Y,Z axis) coordinates in an automated system that covers Z space from ground level to 20,000 feet and X space of maximum 10 miles and Y space by 10 miles maximum.

- 3) DDS logic environment covers all type of behaviors, such as velocities from 1 to 100+ meters/second (m/s).
- 4) DDS does not rely on size to determine the ID of hostile drones and tag them. It focuses on the drone speed zone of 87.0 knots (100 mph) max.
- 5) DDS does not rely on material compositions of the hostile drones to ID and tag them.
- 6) DDS identification, tracking, tagging, and countermeasures functions may be configured to cover or apply to all drones regardless of whether they are commercial models or custom made. All drones have a unique identifier, such as a media access control (MAC) address, that can be determined or read by the DDS and used to identify the drone.
- 7) DDS may be configured to track, tag, and engage countermeasures that can go as far out as 10 miles, 5 miles, or 1 mile with a kill zone in each segment.
- 8) DDS uses many elements that track GPS of all drones.

[0014] In one embodiment, the DDS consists of an electronic remote monitoring device, a classified firmware, different antennas from wireless to satellite depending on what the facilities require and the required area coverage, and a classified software that has an interactive GUI which can communicate with any device and any Internet-enabled (IoT) system. It will function on a Wi-Fi network, so the DSS may interface with a secure network. Antennae may be positioned unobtrusively throughout a facility to provide full communications coverage. The DDS may be configured to communicate via a secure, encrypted Internet cloud-enabled connection to local and national databases, a facility security system, and law enforcement entities. DDS is highly adaptive. The DDS system can be

configured on an available facility's infrastructure. The DDS can be customized for specific needs of a particular user.

[0015] In some embodiments, the DDS constantly scans and surveys WIFI, RF, and sensor signals and processing an auto-logic: An 'if-then' logic may be used to determine different solutions in relationship to the threat.

[0016] The DDS monitors all signals and distinguishes between non-drones and UAV or UAS. In one embodiment, all tracked drones are considered rogue. All drones with definable MAC addresses are tagged by the DDS. All non-MAC address drones activate the countermeasures system.

[0017] DDS Tags all drones and does a MAC address check at the local and national registry. If no MAC address is detected, or if it is not registered, the DDS activates the countermeasures system. All drones MAC addresses are recorded at the national and local registry. In one embodiment, MAC addresses are checked at the tracking and tagged Stages at 10 and 5 mile marks. Untracked drones that show up under the 5 mile mark may activate the countermeasure system. Only drones registered on the local registry as 'friendly' or 'authorized' will allowed to travel from x miles marks to point zero.

[0018] In some embodiments, the countermeasures system is activated under the following conditions or scenarios:

- 1) Rogue drones are processed by a auto-logic 'if/then' logical process which defines, tracks, and tags a drone as hostile or friendly. Activation may occur when the auto-logic intellectual format is triggered by the drone that is hostile or a 'friendly' or 'authorized' drone that has turned hostile.
- 2) Drones are considered unauthorized or hostile if they have no registration from their MAC addresses.

- 3) Drones are considered hostile and activate the countermeasures system if they have a MAC address but it's not registered with the local registry or no MAC address and has crossed the 5 mile safe zone.
- 4) The DDS countermeasure system may be embodied in firmware with firewall systems. The countermeasure system may also involve a custom AES algorithm, 256 key length that deploys different types of defenses in destroying the drone vehicle, interrupting flight, controlling flight, returning to the user/sender of the drone for apprehension, and submitting an electronic record for results for the infractions.

[0019] In some embodiments, the DDS constantly scans and survives signals and processing intruder attempts to hack into the DDS. A DDS hacker format may be provided within the system to answer hacker attacks and attempts to disrupt intrusion activities.

[0020] The DDS may also comprise multiple micro towers or tower implementation to existing towers that are stationed at 10 mile mark, 5 mile mark, and 1 mile mark.

[0021] The multiple micro towers that are stationed at 10 mile mark, 5 mile mark, and 1 mile mark may comprise satellite systems that incorporate a remote device and monitoring control of the WiFi towers and its sensors.

[0022] A hacker response may be built into the system to intercept different types of intrusions and tag, trace, and destroy the intrusion element at the local and remote levels.

[0023] The DDS may be provided with an extensive multi-sensor system to further add to the logic algorithms in tracking and intercepting rogue drones.

[0024] The DDS may also be provided with a display system and a graphic user interface (GUI) to give a visual representation of events that are occurring.

[0025] Having herein set forth preferred embodiments of the present invention, it is anticipated that suitable modifications can be made thereto which will nonetheless remain within the scope of the invention.

ATTACHMENT A

Drone Defense System is a Remote Transmission Security System (Devices and Applications) that saves lives, protects properties, provides security, and engages any unauthorized Drone.

Purpose of Our Invention

Unmanned aerial vehicles UAVs and UAS, better known as drones, are one of the technological marvels of our age. But due to non-regulation and under-regulation, Drones have become a safety hazard and a terrorist aerial stealth weapon.

1.) Air Safety

A growing number of drones have been flown dangerously close to commercial aircraft, violating federal rules for their operation. 25lb to 55lb UAV (Drones) have come close to bringing down airplanes. An air collision with a UAV will be catastrophic loss of life. According to the FAA, more than 650 pilots have reported seeing unmanned aircraft as of Aug. 9 2015, compared to a total of 238 such sightings for all of 2014.

2.) Regulation

Only 36 states out of 50 states have introduced legislation to protect individuals from drone-related privacy invasion issues, but there are serious regulatory inconsistencies for how to address UAV intrusion on privacy, penalties for cost of life from UAV, avoidance of collision, how to protect lives, and countermeasures for Rogue Drones. Only 17 states have passed laws restricting drone usage. And on the federal level, the FAA has unable to publish its plans for the "safe integration" of drones into U.S. airspace.

3.) Flying Weapons

UAVs (Drones) are easy to weaponize. They're being weaponized with everything from pistols to AK-47 machine guns to missile launchers. The weaponization can reach the level of carrying Weapons of Mass Destruction (WMD) into very public areas undetected and non-defended. Drones will become the terrorist prime weaponry. There is no defense for these types of weaponry or detection, since Satellites cannot currently detect them and there are no other consistent, comprehensive methods of detection at this time to prevent mass destruction.

4.) Insurance

The potential legal issues, combined with the uncertain regulatory atmosphere in the U.S., make insurance underwriting for drone liability a challenging endeavor, also a challenge to mitigate aviation liability.

5.) Crowded Skies

Experts say major issues for UAV Traffic control will not be set or developed by the time major Fortune 500 companies start delivering packages via commercial drones - creating congestion in the sky and increasing mid-air collision probability with over-25lb cargo hurling down to earth tearing into houses, killing or hurting people, and causing property damage to name a few scenarios.

Our Drone Defense System (DDS) solves the problem described above.

Drone Defense System is a Remote Transmission Security System that protects life, property, privacy, and security from Intruding Drones (UAV) & (UAS) in unauthorized air space or locations. It resolves the 5 problem areas with Drones:

1.) Air safety

Drone Defense System (DDS) answers the growing number of drones that have been flown dangerously close to commercial aircraft and other rogue Drone activities that violate federal rules for their operation. The DDS Remote Transmission Security Systems (RTSS), code named, "Return to Sender", Detects, Records, Tracks, Targets, Counter Measures, Tags and Intercepts/Control the Rouge drone from 10 meters to 100,000 meters from the threatened object. Different type of countermeasures will be deploy according to the rule of engagement pertaining to the specific DDS Model.

2.) Regulation

The DDS will enable the FAA to create broader regulations with stronger applications that regulate the different Drone systems, from hobbyists, commercial, academic, research/development and Enterprises (Boeing, Lockheed and others). DDS will enable creation of a National Registry for a Cloud based highly secure DDS Database that interacts with the DMV for classification, registration, and recording the signature ID of a Drone and its MAC address (MAC addresses are like the VIN Numbers on vehicles). The DDS would cross-check Drones being tracked for authentication and verification via the DMV and DDS Database that transmits to DDS "RTSS" to activate an action; DDS process will regulate UAV intrusion on privacy, penalties for cost of life from UAV, or avoidance of collision, how to protect lives, and countermeasures from a Rogue Drone.

3.) Flying Weapons

DDS through "RTSS" will apply countermeasures to destroy or control the weaponized drone by returning the Rogue Drone back to the sender and controller, recording and using the Drones resources to ID the owners and destroy or capture the rogue pilot. If there is no GPS return-home behavior activated, the drone will be forced to land, it will be Electronic or RF jammed and disarmed in flight. DDS will be intricately integrated with Law Enforcement entities, and Military/National Guard.

4.) Insurance

The DDS will aid Insurance companies to create intricate insurance policies and real time application to report incidents that are occurring or that have occurred. The insurance would provide coverage similar to car insurance. To enable increasing safety, any drone without registration and insurance will not be allowed to fly or it will be forced to land and be confiscated. DDS insurance format is for additional vetting of the drones in flight via the DMV Database. DDS will be able to construct the format similar to having registration and Insurance when you drive a car that is attached to VIN number of the car.

5.) Crowded Skies

DDS via "RTSS" will be able to regulate flight with a Flyway systems (Imagine an Aerial Highway with GPS and Anti-Collision sensors), DDS will be located in many facilities, where each facility becomes a moderator and traffic controller of Drone flight and it talks to the DDS traffic controller computer/cloud server via a Satellite system that creates specific direction to each Drone via GPS switching flight path routes that are the least congested on the Flyway.

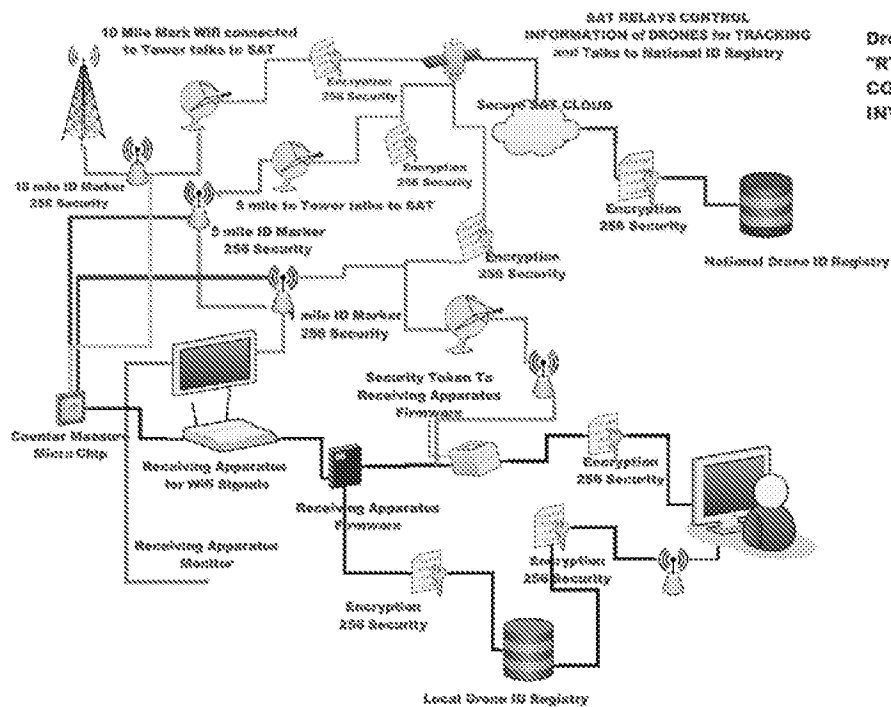
Our Drone Defense System is an Improvement in the following way:

A.) Defense Drone System is different from and better than anything that exists in its field: because it saves lives, it protects properties, it protects privacy, and it protects our National Air Space from Rogue UAV and UAS (Drones).

B.) The problems with the other devices or systems in the field of our invention is the existing "Defense" type systems for Drones fall short in protecting National Air Space, protecting lives, protecting properties or defending against terrorists. From video sensor, or sound sensor, non-countermeasure or Artificial Fencing falls short in the protection of the events listed above.

C.) The reason these devices or systems don't work well is that for a defense system to defend against Rouge drones, it needs to have the ability to protect, countermeasure, ID from a National Database, and to prevent intrusion. Neither the video sensors, sound sensors, infrared sensors, thermal sensors, virtual non-countermeasure domes and the virtual Fencing do not provide the ability to stop the ability to cause harm above. None of the current solutions answer the 5 Drone Problems and issues well enough or comprehensively enough to create Safety.

D.) Drone Defense Systems improves on any system by defending against Rogue Drones, by implement an ability to ID all the Drones from 10 meters to 100,000 meters via an array that IDs all individual MAC addresses and according to the rules of engagement (these rules can be customized for any protected area) it creates a countermeasure that will disarm, intercept, Return to Sender, or force land a rogue drone.



Drone Defense SYSTEM
"RTS" REMOTE RETURN SECURITY SYSTEMS AND DEVICES
CODE NAME: "RETURN TO SENDER"
INVENTORS PETER WHITMARSH AND SHANA WHITMARSH

Color Processing Keys

- Encrypted Closed Communication and Monitoring
- ~~~~~ Encrypted Counter Measure Executed
- Encrypted Counter Measure Trigger
- ~~~~~ Encrypted Remote Security Transmission of Data and Tracking of Drone ID
- ~~~~~ Encrypted Closed Relay of Drone Data and Registry.

Components of RTS

- | | | |
|---|--|--|
| Wireless Apparatus Receiver | Wireless Receiving Apparatus Logic Registry Database | Wireless Receiving Apparatus WDR, RF, and multi-sensor tower |
| Wireless Receiving Apparatus Firmware | Closed Cloud National Drone Registry Database | Wireless Receiving Apparatus Dedicated SAT |
| Counter Measure Chip | Wireless Receiving Apparatus WDR Relay System | Wireless Receiving Apparatus closed communication cloud |
| Wireless Receiving Apparatus Monitor | Wireless Receiving Apparatus 256 encryption keys | Wireless Receiving Apparatus Operator |
| Wireless Receiving Apparatus Security Token | Wireless Receiving Apparatus SAT System | |

The diagram illustrates a network architecture with several interconnected components:

- WGS/KF/Genev**: Located at the top left.
- 10 955 Zone**: Located below WGS/KF/Genev.
- 5 acio zone**: Located in the middle left.
- 2 mly zone**: Located at the bottom left.
- Database Registry of Mac Addresses**: Located at the bottom center.
- Threats**: Located near the Database Registry.
- Input DNS Access Priority**: Located in the center.
- clouded cloud network**: Located above Input DNS Access Priority.
- National DNS Database Registry**: Located to the right of the clouded cloud network.
- Access**: Located further right.
- Random keying to increase DNS**: Located below Access.
- Return to Sender Message Database**: Located at the bottom right.
- New Top Net IPV2 entry**: Located at the very bottom.

Dashed lines represent connections between these components, forming a complex web of interactions.

- Anger Being Tracked and ID
- Anger Being Tracked
- Anger Counter Modifying Responses
- Anger ID as Priority No Action

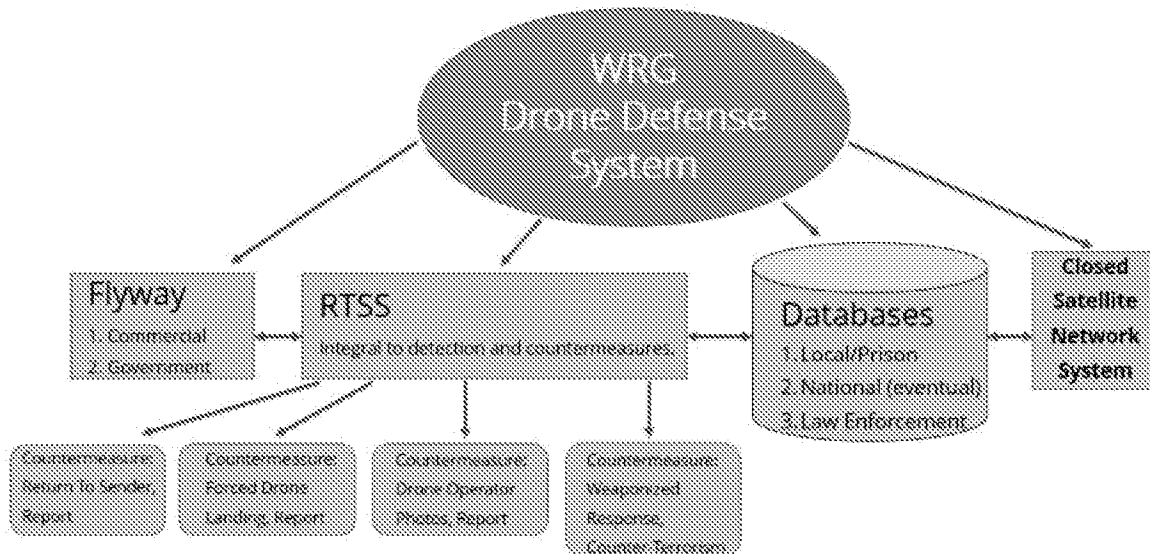
- AXON EXHIBIT 1006, Page 25

Remote Transmission Security System and Device – “Return to Sender”

Drone Defense System is a Remote Transmission Security Device and Application that saves lives, protects properties, provides security, and engages unauthorized Drones.

UAVs (Drones) are being weaponized with everything from pistols to AK-47 to missile launchers and the threat is very serious since drones can just as easily be equipped with weapons of mass destruction (WMD) and flown into public areas undetected and non-defended. Drone use will become the terrorist's primary choice for weaponry. There is currently no true defense against this kind of weaponry and there is no reliable detection, since air traffic control systems and Satellites presently cannot detect them and there are no other detection systems at this time that are sensitive or responsive enough to prevent individual threats or attempts at terrorism or mass-destruction.

WRG Drone Defense System (DDS) – An Overview



Electronic Patent Application Fee Transmittal

Application Number:				
Filing Date:				
Title of Invention:	UAV DEFENSE SYSTEM			
First Named Inventor/Applicant Name:	Peter Whitmarsh			
Filer:	Bruce E. Dahl/Cynthia Sullivan			
Attorney Docket Number:	WHIT US-1PRV(040492.0002)			
Filed as Small Entity				
Filing Fees for Provisional				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Provisional Application Filing Fee	2005	1	130	130
Pages:				
Claims:				
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 (\$)				130

Electronic Acknowledgement Receipt

EFS ID:	24363257
Application Number:	62267393
International Application Number:	
Confirmation Number:	9782
Title of Invention:	UAV DEFENSE SYSTEM
First Named Inventor/Applicant Name:	Peter Whitmarsh
Customer Number:	27104
Filer:	Bruce E. Dahl
Filer Authorized By:	
Attorney Docket Number:	WHIT US-1 PRV(040492.0002)
Receipt Date:	15-DEC-2015
Filing Date:	
Time Stamp:	12:43:05
Application Type:	Provisional

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$ 130
RAM confirmation Number	12044
Deposit Account	060590
Authorized User	DAHL, BRUCE E.

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

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 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	Application Data Sheet	aia0014-WHIT_US-1PRV.pdf	1854042	no	8
			b3291c263747bbb588cc431e27c610d80dc746c5		
Warnings:					
Information:					
2	Specification	Patentapplicationprv.pdf	43214	no	9
			ff74a2402105dc4735fe45f81fc217dd87418a29		
Warnings:					
Information:					
3	Appendix to the Specification	AttachmentA.pdf	3095642	no	6
			e3893a56464044d11e8823a681653de7de732900		
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	30009	no	2
			e983cd3fec375bca77f4addf1a856ba1458ea115		
Warnings:					
Information:					
Total Files Size (in bytes):			5022907		

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.