Ex. A6

Claim Chart for U.S. Patent No. 8,234,704 – Combination References[1]

Each of the following references qualifies as prior art to the asserted claims of the '704 patent (claims 11, 12, 13, 14, and 15) under 35 U.S.C. §§102-103 in view of its applicable filing and/or publication dates:

References	Shortname
Smart Card Alliance, Using Smart Cards for Secure Physical Access, ID-03003, July 2003	Using Smart Cards
U.S Pub. App. No. 2002/118096A1	Hoyos
U.S. Pub. App. No. 2006/123229A1	Holloway
U.S. Patent No. 7,437,755 B2	Farino
U.S. Pub. App. No. 2006/0242116A1	Ahmed
U.S. Pub. App. No. 2003/0206100A1	Richman
U.S. Pub. App. No. 2007/083915A	Janakiraman
U.S. Pub. App. No. 2003/005326A1	Flemming
U.S. Patent No. 7,296,070 B2	Sweeney
U.S. Pub. App. No. 2009/0320088A1	Gill
U.S. Pub. App. No. 2006/0268758A1	Serani
U.S. Pub. App. No. 2007/0030120A1	Gusse
U.S. Patent No. 7,624,422 B2	Williams
U.S. Patent No. 7,280,030 B1	Monaco
U.S. Pub. App. No. 2007/0174907A1	Davis

[1] Identified herein are exemplary portions of the references based on presently available information and Plaintiff's current allegations. The references, however, may contain additional support for particular claim limitations. Defendant expressly reserves the right to rely on uncited portions of the prior art references, other documents subject to discovery, and Defendant's expert reports to provide context and/or to aid in understanding the cited portions of the references. In instances of cumulative disclosure within a particular prior art reference, Defendant may have cited a subset of those instances as opposed to citing each instance; however, Defendant reserves the right to rely on uncited instances of cumulative disclosure. Where Defendant cites to a particular figure in a reference, the citation should be understood to encompass the caption and description of the figure and any text relating to or discussing the figure. Conversely, where Defendant cites to particular text referring to a figure, the citation should be understood to include the figure as well. The citations included herein disclose the claim elements either expressly or inherently.

HID Ex. 2004 – Page 1
Vector Flow Inc. v. HID Global Corp.
IPR2023-00353 – Pat. No. 8,234,704

As set forth in the chart below, all Asserted Claims are anticipated and/or obvious over this reference alone or in view of the other references cited in Defendant's Invalidity Contentions and the knowledge of a person of ordinary skill in the art.

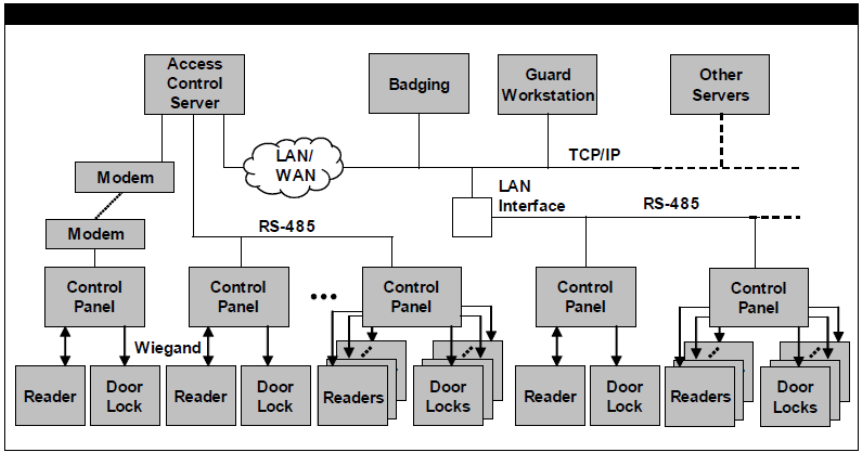
Except where specifically noted otherwise, this chart applies the apparent constructions of claim terms as used by Plaintiff in its infringement contentions; such use, however, does not imply that Defendant adopts or agrees with Plaintiff's constructions in any way.

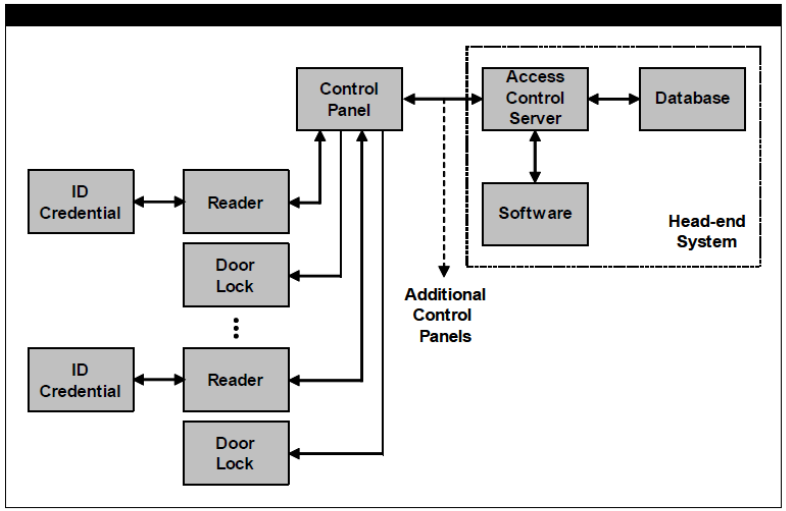
To the extent the charted reference is held not to explicitly or inherently disclose any particular element below, such limitations were obvious in view of the disclosures cited below and the reasons and disclosures of other references as set forth in Defendant's Invalidity Contentions, which are incorporated herein by reference.

Defendant is investigating the prior art and has not yet completed discovery. Defendant reserves the right to modify, amend and/or supplement these contentions as information becomes available, and as discovery proceeds.

Element	Asserted Claims	References
Claim 11		
11(pre)	A method comprising:	"The present invention relates to a multiple site integrated security system method and communications protocol." Richman at [0003]
11(a)	interfacing in a centralized security system, a plurality of security sensor types distributed throughout a plurality of sites, each sensor type configured to respond to a corresponding type of actionable event, each sensor type provided by a different manufacturer of a plurality of manufacturers;	Using Smart Cards, e.g., Figs. 1 and 3 and associated text (describing interfacing multiple sensor types which may be associated with multiple sites such as buildings and other spaces)

HID Ex. 2004 – Page 2
Vector Flow Inc. v. HID Global Corp.
IPR2023-00353 – Pat. No. 8,234,704

Element	Asserted Claims	References
		Figure 3: Example of Networked Physical Access Control System 

Element	Asserted Claims	References
		Access Control System Components A typical access control system is made up of the following components: • ID credential (smart card) • Door reader (smart card reader[1]) • Door lock • Control panel • Access control server • Software • Database Figure 1 illustrates how these basic components interconnect, with each component described in the following sections. **Figure 1: Access Control System Schematic**  [1] Smart card "readers" can both read and write to a smart card. Referring now to FIG. 1, there is shown generally a security system 10, an administration system 12, and a database integration platform 14 according to one embodiment of the present invention. **Security system 10 is an access control system such as the B.A.S.I.S.® System sold by Best Access Systems® of Indianapolis, Ind., a business unit of Stanley® Security Solutions.** As shown in FIG. 2, security system 10 generally includes a server computing device 16, such as a workstation

HID Ex. 2004 – Page 4
Vector Flow Inc. v. HID Global Corp.
IPR2023-00353 – Pat. No. 8,234,704

Element	Asserted Claims	References
		or personal computer, having a user interface 18, a display 20, software 22, and a security database 24 (also shown in FIG. 1), **a plurality of access control panels 26 disposed at various locations throughout controlled areas of the facility, and one or more badge reader/door lock units 28 associated with each of panels 26.** As is described in greater detail below, **a user (e.g., a student) gains access to an area (e.g., a dorm room) by presenting his identification badge (not shown) to unit 28, which in turn verifies that the student associated with the badge has sufficient access rights (as reflected by data stored in security database** 24) to enter the area, and electronically unlocks the door. An administrator of security system 10 uses computing device 16 to, among other things, assign access rights to users based on the requirements of the particular enterprise." Holloway at [0017]. "The **program 300 includes an Event Management Program (EMP).** The system monitors activities of the LAN and the client PCs in real-time using an Event Management Program (EMP) stored on an Administrative user's PC to record 'events'. The EMP is an object oriented program having a number of modules for performing discrete tasks during monitoring of the client PCs activities resulting from interaction with a client PC user. The **EMP receives event data from Agent software programmed into each client PC (or other network appliance).** The Agent software includes Application Agent Modules (AAMs), System Agent Modules (SAMs) and the operating system's Application Program Interface (API) for each client PC. Event data for each PC is monitored by the AAMs, SAMs and API activities as PC user's interact with their respective PCs. The event data is passed onto an Object Request Broker (ORB) module located on an Administrative user's PC, which acts as a register when users activate particular applications on their client PC's. The ORB directs messages to and from the EMP as appropriate. If the ORB

Element	Asserted Claims	References
		determines that particular event data should be recorded in the event management program, it passes the event data onto the communications handler module (CHM)." Sweeney at [5:31] "**Event data can be received from a number of event data sources as users interact with their PCs or when the PCs** and hence the LAN generate events. Event data sources include the network transport layer, security layer, and PC application programs and operating systems. **Each of these event data sources may produce data in a unique format dependent upon the application or system** being monitored. **The EMP therefore includes a Universal Parser Module (UPM) which reads event data from the EMP in its original format and converts the original format into a common data format (CDF)** for storage in a relational database." Sweeney at [5:54] Sweeney at [9:3] Sweeney at [9:53] Sweeney at [12:1] "The **EMP 310 is very flexible and can be implemented in a number of applications.** For example, **other applications may relate to security systems of the business organisation**, in which hacking attempts to the LAN **12** can be recorded and suitable action taken. Or alternatively, an organisation's telephone system can be monitored to determine the frequency of particular phone calls that an employee makes from their telephone. Additionally, the **EMP 310 can be connected to the physical security system of the organisation's premises and issue appropriate**

HID Ex. 2004 – Page 6
Vector Flow Inc. v. HID Global Corp.
IPR2023-00353 – Pat. No. 8,234,704

Element	Asserted Claims	References
		alerts by paging security personnel and management of a break-in attempt." Sweeney at [12:66] "A **security access control system includes a plurality of security access control devices at respective physical access points for controlling physical access thereat.** Each **security access control device includes a wireless transnsceiver and a controller cooperating therewith a establish a wireless ad hoc network among the plurality of security access control devices.** A host control station includes a wireless transceiver and a host controller cooperating therewith to communicate to at least one of the security access control devices via the wireless ad hoc network." Gusse at [Abstract] "At **least one of the security access control devices transmits status data to the host control system via the wireless ad hoc network.** The status data may comprise at least one of battery status, user status, and security access control device operating status. The status data may be transmitted in real time. **The security access control device operating status may comprise at least one of an unlocked state, a card controlled state, an access disabled state, and a dual mode state.** In addition, the status **data may comprise audit data, wherein the audit data includes system events, access attempts by a user, and a time and access event outcome of the access attempts made by the user**." Gusse at [0013] "Referring initially to FIG. 1, **a security access control system 10 comprises a plurality of security access control devices 20(1)-20(*n*) at respective physical access points 22(1)-22(*n*) for controlling physical access thereat.** A physical access point **22**(**1**)-**22**(*n*) may be any area in which entry by a user needs to be controlled and

HID Ex. 2004 – Page 7
Vector Flow Inc. v. HID Global Corp.
IPR2023-00353 – Pat. No. 8,234,704

Element	Asserted Claims	References
		monitored. For instance, the physical access points **22**(**1**)-**22**(*n*) at a university are staff offices, professor offices, lab rooms, supply rooms, etc. These are fixed physical access points." Gusse at [0022] "FIG. 6 illustrates one embodiment of the present invention where a unified access control server 200 for network and physical premises access is shown. Server 200 interfaces with both the legacy physical security system 202 and the frame/packet network 204 to control a unified physical access and/or network access. This system may be adapted to monitor and control access to buildings, homes, physical infrastructure as well as to information and network systems. Advantageously, server 200 unifies credential verification and associated policies and policy enforcement for physical facilities and network-enabled devices. This unification facilitates implementation of new security policies that strengthens both physical and network security. These policies eliminate security holes in both the physical access control and network access control systems and ensure that both the facility access system and the network access system are diligently monitored and managed." Farino at [10:31] "Therefore, a new and improved computer implemented communications protocol is provided, which is an **XML based communications protocol for security monitoring purposes.** T**his unique XML based communications protocol is implemented through numerous modules which receive and convert data messages from diverse security devices and sensors, standardize and send converted messages, and encrypt and decrypt said data messages as necessary.** With the set modules, the data messages are filtered and transmitted from checkpoint computers to base station computers, which analyzes, reports and logs environmental as well as security events within a subject site. The resulting integrated security system provides better trained security

Element	Asserted Claims	References
		guards, who are more alert and responsive, and more closely supervised and easily scheduled, enhanced financial monitoring, more accurately paid and costed security services, better archived and reported security related events, as well as being better coordinated with public agencies, enhanced safety, and readily upgraded and integrated with existing and future technologies." Richman at [0066] "FIG. 1 thereof, there is shown a new and improved multiple site integrated enhanced human oriented security system 10. Specifically, the multiple site integrated security system 10 as represented by FIG. 1 and constructed in accordance with the present invention, uses direct communication 22 and indirect communication (for example use of a global computer network like the Internet 20) methods of communication between a central headquarters 16 and one or more facilities sites 12 and 14." Richman at [0077] "The new multiple site integrated security system 10 may be tailored to site specific needs or pre-existing hardware and equipment as represented by a Site A security subsystem 12 and a Site B security subsystem 14. The sites may be in communication with the integrated headquarters server subsystem 16 by means of direct communication 22 as exemplified by communication with the Site B security subsystem 14. This direct communication 22 between the sensors and the checkpoint data processing subsystems, and between the checkpoint data processing subsystems and the base station CPUs may also be accomplished through the use of existing electrical power lines located at the guarded facility or site." Richman at [0078]

Element	Asserted Claims	References
		"1. Conversion Module 202. **This module receives data from security hardware devices of varying types in their own specialized unique data format and converts this data into a standardized XML formatted message.** Each unique hardware device requires a separate customized conversion module to translate its data into the coded SCA XML format for the purpose of further analysis. Thus, for this module, the input is a varying hardware signal, and the output is a standardized message in XML format." Richman at [0097]
11(b)	accepting sensor data from each security sensor an integration module including an agent for each type of security sensor, wherein the sensor data from each security sensor is embodied in a native data representation format of each respective manufacturer of the plurality of manufacturers;	Using Smart Cards, e.g.: The access control system's data format is a critical design element. Data format refers to the bit pattern that the reader transmits to the control panel. The format specifies how many bits make up the data stream and what these bits represent. For example, the first few bits might represent the facility code, the next few a unique credential ID number, the next few parity, and so on. Many access control system vendors have developed their own formats, making every vendor's coding unique. Like the pattern of teeth on a door key, the formats are kept secret to prevent an unauthorized person or company from duplicating a card. Existing installed access control system formats must be considered when defining the requirements for implementing new physical access control system technologies. "An embodiment of the system of the **present invention may also include a data collector interface for coupling external data sources to the database.** The **data collector interface converts data from the native format for an external data source to one that is compatible with the structure of the database in which the data is stored**. This data conversion function of the data collector interface enables the database or databases of the present invention to be coupled to a plurality of external data sources without requiring that all of the

Element	Asserted Claims	References
		external data sources conform to one particular database structure. Furthermore, the data collector interface includes transaction services that generate the instructions for a database API that are required to store the data in the database. **Thus, data sources from diverse locations may be coupled to a database at a common site**. Consequently, a significant accumulation of historical data may be obtained for a data mart component of the database, which further enhances the value of the data mining applications at the common site. However, the data provider interface also supports the segregation of the collected data into different databases so control application programs may be developed from the data originated at the particular building site for which the application is being developed." Ahmed at [0029] "Therefore, a new and improved computer implemented communications protocol is provided, which is an **XML based communications protocol for security monitoring purposes.** T**his unique XML based communications protocol is implemented through numerous modules which receive and convert data messages from diverse security devices and sensors, standardize and send converted messages, and encrypt and decrypt said data messages as necessary.** With the set modules, the data messages are filtered and transmitted from checkpoint computers to base station computers, which analyzes, reports and logs environmental as well as security events within a subject site. The resulting integrated security system provides better trained security guards, who are more alert and responsive, and more closely supervised and easily scheduled, enhanced financial monitoring, more accurately paid and costed security services, better archived and reported security related events, as well as being better coordinated with public agencies, enhanced safety, and readily upgraded and integrated with existing and future technologies." Richman at [0066]

Element	Asserted Claims	References
		"FIG. 1 thereof, there is shown a new and improved multiple site integrated enhanced human oriented security system 10. Specifically, the multiple site integrated security system 10 as represented by FIG. 1 and constructed in accordance with the present invention, uses direct communication 22 and indirect communication (for example use of a global computer network like the Internet 20) methods of communication between a central headquarters 16 and one or more facilities sites 12 and 14." Richman at [0077] "The new multiple site integrated security system 10 may be tailored to site specific needs or pre-existing hardware and equipment as represented by a Site A security subsystem 12 and a Site B security subsystem 14. The sites may be in communication with the integrated headquarters server subsystem 16 by means of direct communication 22 as exemplified by communication with the Site B security subsystem 14. This direct communication 22 between the sensors and the checkpoint data processing subsystems, and between the checkpoint data processing subsystems and the base station CPUs may also be accomplished through the use of existing electrical power lines located at the guarded facility or site." Richman at [0078] "The checkpoint data processing subsystems 40 and 50 then process all of the information gathered from any peripheral equipment as exemplified by 42, 44, 46, 48, 52, 54, 56, and 58, and transmits the event sensor information to the base station computer or CPU 30. The base station computer or CPU 30 accepts information from all checkpoint data processing subsystems 40 and 50, and any others in communications therein, stores the information in a database 34, provides access to this

HID Ex. 2004 – Page 12
Vector Flow Inc. v. HID Global Corp.
IPR2023-00353 – Pat. No. 8,234,704

Element	Asserted Claims	References
		information to personnel in real-time mode and generates alerts if indicated by alert logic." Richman at [0081] "1. Conversion Module 202. **This module receives data from security hardware devices of varying types in their own specialized unique data format and converts this data into a standardized XML formatted message.** Each unique hardware device requires a separate customized conversion module to translate its data into the coded SCA XML format for the purpose of further analysis. Thus, for this module, the input is a varying hardware signal, and the output is a standardized message in XML format." Richman at [0097] "Legacy physical security device access gateways, such as shown in FIG. 3, block 125, are available that can translate various access control system device vendor's signaling formats and protocols to another access control system vendor's component formats. These gateways provide greater interoperability between disparate physical security vendor system components and may allow physical security information to be transported over a frame/packet based network" Farino at [8:59]
11(c)	defining individual user profiles and their respective access privileges and credentials in the system;	"Devices and systems for the provision of safety and security of persons and property are well known. Examples of different types and kinds of security systems for protection and surveillance methods of building structures and surrounding areas are disclosed in U.S. Pat. Nos. 6,204,762 B1, 6,154,133, 6,097,429, and 5,825,283. In general, the structure and function of most security systems involves electronic surveillance equipment monitored at a centralized location. Current development of security systems attempts to do away with

HID Ex. 2004 – Page 13
Vector Flow Inc. v. HID Global Corp.
IPR2023-00353 – Pat. No. 8,234,704

Element	Asserted Claims	References
		human-oriented services and replace the human security guard with high technology solutions to security problems. Only a limited number of currently developed security systems utilize a combination of guards in close conjunction with the electronic equipment. Most of the time, these systems involve one guard who monitors a video feed or alarm panel for intrusion or other related alerts. These security systems are commonly built, installed and implemented without any regard for the particular facilities of other systems, for example, the facilities of built-in environmental and climate control, the tracking of people and assets within the building or complex, and fire/smoke detection as well as transport systems such as elevators, etc. Therefore, it would be highly desirable to have a new and improved security system which not only enhances the human security guard services, but also integrates facilities management, and allows for identification and global positioning satellite (GPS) tracking of people as well as assets such as computers, and other valuable instrumentation, all in a readily scalable configuration utilizing off the shelf electronic security and communications components." Richman at [0006]-[0008] "Still another object of the instant invention is to provide a system for security which monitors the identification and authorization of personnel inside secured areas through use of a two points access subsystem composed of a fixed device installed at a checkpoint and a mobile device (wearable or hand held) carried by authorized personnel which could be configured to integrate pre-existing security systems without modification of the core program." Richman at [0051] "A schematic diagram of checkpoint computer communications options 70 is illustrated in FIG. 4. Another embodiment of a checkpoint computer

HID Ex. 2004 – Page 14
Vector Flow Inc. v. HID Global Corp.
IPR2023-00353 – Pat. No. 8,234,704

Element	Asserted Claims	References
		72 receives and records information from peripheral event sensor equipment. Most of these devices, such as an access control system 94 coupled with a motion detection device 74, an identification or ID tracking device 76, an GPS tracking system or tracking device 78, a temperature sensor 96 coupled with a fire and smoke detection device 82, perimeter control systems 98, a hand held device 84 such as various security guard communications equipment or a PDA-type device, video camera subsystems 86, climate control subsystems 88 such as heating ventilating and air conditioning (HVAC) subsystems, and transport subsystems 92 such as elevator control device, will all send information instantly and simultaneously to the checkpoint computer 72 by means of a security system communications protocol through an embedded Input/Output (I/0) microprocessor, as shown within the checkpoint computer 72." Richman at [0084] "According to one aspect of the invention a security system includes a first and second unit. The first unit generates a database of biometric features each associated with a specific person. To create this database, the first unit uses an input that generates an electronic representation of a biometric feature." Hoyos at [0007] "According to a further aspect of the invention, the security system also includes a third unit operationally coupled with the second unit. The second and third unit are situated on opposite sides of the access point, such as a door. The third unit includes an input configured to generate an electronic representation of the biometric feature. This input is operationally coupled with the computer processor of the second unit. When this computer processor receives an electronic representation of the biometric feature from the input device of the third unit it compares it

Element	Asserted Claims	References
		with the database of biometric features to determine whether the comparison generates a match. If so, it opens the access point." Hoyos at [0008] Hoyos at [0012] "According to a further aspect of the invention, the **remote computer determines access privileges after generating a match with the biometric feature and the user ID.** The remote computer unlocks the access mechanism only if the user has access privileges." Hoyos at [0028]. "In an alternative preferred embodiment, **a particular user may be given access permission only to certain access points.** In this configuration, the respective remote computer will also check for access privileges. If the user does not have access privileges for the associated access point, then the remote computer will not permit access through that access point. For example, **a user may have access privileges for the access point associated with remote computer 120 and user interface 132, but not for any other access point.** In this configuration, when the user is properly identified at the access point then he or she will be permitted to pass through the access point. However, when the user attempts to access any other access point, the user will be advised that he or she does not have privileges for that access point." Hoyos at [0053]. Flemming at [0043]–[0044], [0047] "The unified access control server 200 eliminates the need for an Access Control Panel and a network access control server while

HID Ex. 2004 – Page 16
Vector Flow Inc. v. HID Global Corp.
IPR2023-00353 – Pat. No. 8,234,704

Element	Asserted Claims	References
		maintaining the valid credential list and access policies in a table previously supported by these devices" Farino at [10:49] Janakiraman at [0035]
11(d)	mapping the sensor data from each security sensor in the native data representation format of each manufacturer of the plurality of manufacturers to a common data representation format, the common data representation format including a data object and processing information for the sensor data;	"Therefore, a new and improved computer implemented communications protocol is provided, which is an **XML based communications protocol for security monitoring purposes.** T**his unique XML based communications protocol is implemented through numerous modules which receive and convert data messages from diverse security devices and sensors, standardize and send converted messages, and encrypt and decrypt said data messages as necessary.** With the set modules, the data messages are filtered and transmitted from checkpoint computers to base station computers, which analyzes, reports and logs environmental as well as security events within a subject site. The resulting integrated security system provides better trained security guards, who are more alert and responsive, and more closely supervised and easily scheduled, enhanced financial monitoring, more accurately paid and costed security services, better archived and reported security related events, as well as being better coordinated with public agencies, enhanced safety, and readily upgraded and integrated with existing and future technologies." Richman at [0066] "Site specific communication protocols, to collect data from sensors, will be developed and deployed for each project. The universal communications protocol, comprised of an encrypted XML-enabled proprietary software program, will direct communications between the checkpoint data processing subsystems or checkpoint computers and the base stations as well as any headquarters servers deployed within the system (see FIG. 5 and FIG. 6 below).

HID Ex. 2004 – Page 17
Vector Flow Inc. v. HID Global Corp.
IPR2023-00353 – Pat. No. 8,234,704

Element	Asserted Claims	References
		FIG. 5 is a block diagram of a checkpoint computer hardware architecture in greater detail 100. The CPU microprocessor controller 102 converts the incoming and outgoing signals by means of application software which is stored in the memory (ROM and RAM) 104 of the checkpoint." Richman at [0085]–[0086] "Turning now to FIG. 6, there is illustrated a block diagram of an integrated security system encrypted XML communications protocol 120 exemplifying communications between checkpoints and the system core application at a base station, as constructed in accordance with the present invention. The system sensors 122 communicate any (and all) system event 124 to a checkpoint 130 via a custom protocol." Richman at [0086] "The attribute code(s) and value(s) 136, together with associated sensor code 132 and event code 134 for a given system event 124, are detected and processed by the checkpoint encrypted XML communications protocol software which generates the encrypted XML message which can then be transferred over the network, LAN or a global computer network such as the Internet." Richman at [0089] "Referring now to FIG. 7, in operation, under Level I 190, security devices and sensors transmit data in device language specific for that device or sensor. Under Level II 192 a checkpoint data processing unit collects data messages from various site security devices and sensors in unique device language and translates these messages into standardized messages to be passed on to the SCA. This is accomplished by generating a message based upon converted coded data messages and transmitting the converted messages to computers containing the SCA. Under Level III 196, base station computers and/or off site headquarters computers, or any other off site computers (such as remote workstations),

Element	Asserted Claims	References
		analyze the coded transmitted messages whereby such analysis is used to generate reports and logs for the purpose of effectively monitoring the environmental and security conditions within a subject site." Richman at [0092]–[0093] "Therefore, Level I 190 operations include data transmission from any number of existing, or yet to be created, security devices and event sensors, either off the shelf units and/or customized combinations, all having their own specialized and unique device language transmitting components and qualities. In this regard, the present invention can be programmed to receive all of the data message formats originating from any and all of these devices, then be integrated into any site for security and/or environmental monitoring in a customized and readily scalable fashion." Richman at [0094] "1. Conversion Module 202. **This module receives data from security hardware devices of varying types in their own specialized unique data format and converts this data into a standardized XML formatted message.** Each unique hardware device requires a separate customized conversion module to translate its data into the coded SCA XML format for the purpose of further analysis. Thus, for this module, the input is a varying hardware signal, and the output is a standardized message in XML format." Richman at [0097] "**The generated code by the checkpoint could be encrypted (see security protocol) in order to keep the information undisclosed while it is transferred over the network or internet.** After these 3 elements have been received by the BS, the SCA will process and decrypt the incoming XML code. **The "event code" and "sensor code" will generate an entry in the event log. An SQL trigger or stored**

HID Ex. 2004 – Page 19
Vector Flow Inc. v. HID Global Corp.
IPR2023-00353 – Pat. No. 8,234,704

Element	Asserted Claims	References
		procedure will process the attributes of the event. They will compare the attribute values to the alarm values stored in the database and generate an alarm event accordingly. The alarm event is stored in the alarm log." Richman at [0115] "Legacy physical security device access gateways, such as shown in FIG. 3, block 125, are available that can translate various access control system device vendor's signaling formats and protocols to another access control system vendor's component formats. These gateways provide greater interoperability between disparate physical security vendor system components and may allow physical security information to be transported over a frame/packet based network" Farino at [7:59] "The audit servers 12 are preferably strategically deployed around the global network to gather facts about wired 16 or wireless 22 local networks within the global network. According to one embodiment of the invention, **the audit servers 12 are configured to gather facts relating to the wired and/or wireless 22 local networks using heterogeneous information sources. Such information sources may include scanners, cameras, manually entered data, and/or the like. The data gathered by each information source is converted into a normalized data format, such as, for example, and XML (Extensible Markup Language), and stored in the audit repository 14 for access by the compliance server 10.**" Williams at [04:65] "According to one embodiment of the invention, the scan harness 212 works with one or more scanners 204-210 to launch a pre-configured audit based on the target list created by the topology analytic engine 200 at a pre-determined time as scheduled by the compliance server 10. In

HID Ex. 2004 – Page 20
Vector Flow Inc. v. HID Global Corp.
IPR2023-00353 – Pat. No. 8,234,704

Element	Asserted Claims	References
		this regard, the scan harness 212 provides necessary input to the various heterogeneous scanners 204-210, and receives the scan results that represent the facts gathered about the network as output. **The scan results are often heterogeneous in their format when heterogeneous scanners are used. The scan harness 212 takes the scan results in their heterogeneous formats, and automatically converts them into a single, normalized data format. According to one embodiment of the invention, the normalized data format is a machine-processable language format such as XML, which, according to one embodiment of the invention, is normalized for structure but not for semantic equivalence. According to this embodiment, semantic equivalence normalization is done in the P&V engine 34 (FIG. 2) as is described in further detail below. In making the automatic conversion of the data format structure, the scan harness 212 may utilize a conversion table that maps known fields in the output of a particular scanner into XML fields used in the XML format. The normalization allows the scan results to be consistently parsed and stored in the audit repository 14.**" Williams at [11:57] "Regardless of a method in which the network information is obtained, **each audit server 12 generates a scan results document 220 with scan data that is normalized into a standard XML format. The P&V engine 34 (FIG. 2) resident in the compliance server 10 then applies one or more policies to the scan results.** According to one embodiment of the invention, the pattern matching and transformation aspects of the P&V engine 34 are implemented via an XLST processor conventional in the art." Williams at [15:06]
11(e)	generating unique physical access privileges and credentials to exclusively map a defined	"According to one aspect of the invention a security system includes a first and second unit. The first unit generates a database of biometric

HID Ex. 2004 – Page 21
Vector Flow Inc. v. HID Global Corp.
IPR2023-00353 – Pat. No. 8,234,704

Element	Asserted Claims	References
	user profile to a spatial hierarchy of physical sites along with security devices of the system, wherein the unique physical access credentials maintain a common representation of the user's identity across the plurality of sites and to associate specific user identities with respective actionable events;	features each associated with a specific person. To create this database, the first unit uses an input that generates an electronic representation of a biometric feature." Hoyos at [0007] "According to a further aspect of the invention, the security system also includes a third unit operationally coupled with the second unit. The second and third unit are situated on opposite sides of the access point, such as a door. The third unit includes an input configured to generate an electronic representation of the biometric feature. This input is operationally coupled with the computer processor of the second unit. When this computer processor receives an electronic representation of the biometric feature from the input device of the third unit it compares it with the database of biometric features to determine whether the comparison generates a match. If so, it opens the access point." Hoyos at [0008] Hoyos at [0012] "According to a further aspect of the invention, the **remote computer determines access privileges after generating a match with the biometric feature and the user ID.** The remote computer unlocks the access mechanism only if the user has access privileges." Hoyos at [0028]. "In an alternative preferred embodiment, **a particular user may be given access permission only to certain access points.** In this configuration, the respective remote computer will also check for access privileges. If the user does not have access privileges for the associated access point, then the remote computer will not permit access through that access point. For example, **a user may have access privileges for the access point associated with remote computer 120 and user**

Element	Asserted Claims	References
		interface 132, but not for any other access point. In this configuration, when the user is properly identified at the access point then he or she will be permitted to pass through the access point. However, when the user attempts to access any other access point, the user will be advised that he or she does not have privileges for that access point." Hoyos at [0053]. Hoyos at [0089] Flemming at [0066] "The unified access control server 200 eliminates the need for an Access Control Panel and a network access control server while maintaining the valid credential list and access policies in a table previously supported by these devices" Farino at [10:49] Janakiraman at [0035]
11(f)	defining physical security policies of the site in the context of user profiles at all sites through actionable representations of physical, network and information technology resources of the site, wherein the security policies define standardized rule definitions through visual rules depicted by live objects that contain attributes to define their spatial relationship to the actionable representations, and that are applied to the actionable events normalized to the common data	"FIG. 4 is an exemplary screen shot of a **graphics users interface (GUI) for invoking the policy editing and policy deployment modules 40, 44** according to one embodiment of the invention. The GUI provides an explorer window **72** for navigating the various files stored in the policy library **42**. The **GUI further provides a toolbar 36 with a plurality of selectable menus and submenus for accessing the various functionalities provided by the policy editing and deployment** modules. A work area **37** may be used to generate displays associated with the accessed functionalities." Williams at [7:04] "According to one embodiment of the invention, **a new rule may be created by selecting a new rules option (not shown) from a file**

HID Ex. 2004 – Page 23
Vector Flow Inc. v. HID Global Corp.
IPR2023-00353 – Pat. No. 8,234,704

Element	Asserted Claims	References
	representation format to produce normalized event data; and	**menu 101 of the toolbar 36.** As is illustrated in FIG. 5, selection of this option causes the policy editing module **40** to display a pop-up window **38** requesting the user to provide a name of the new rule as well as a rule type. Selection of an OK button causes the policy editing module **40** to display a rule editor window in the work area **37**." Williams at [7:36] "According to one embodiment of the invention, **a new policy may be created by selecting a new policy option (not shown) from the file menu 101 of the toolbar 36**. As is illustrated in FIG. 7, selection of the new policy option causes the display of a pop-up window **41** requesting the user to provide a name of the new policy as well as the policy category. The user may also optionally provide, at this time, a path to a natural language source document file to be associated with the policy. The user may further select to associate to the policy, a latest version of all available current rules, or rules that are associated with an existing policy." Williams at [8:15] "It is a further object of the instant invention to **provide a system of security which is able to be custom configured and scaled up or down, by being individually tailored to site conditions such as site component configurations, checkpoint locations, building type material, building transportation systems, facilities environmental control systems, such as climate control, fire and smoke detection, and other varied parameters.**" Richman at [0049] "Yet another object of the present invention is to **provide a system which would automatically monitor and control certain movable and fixed site conditions such as people and vehicles** at checkpoints, safety systems, access control systems, **position sensors,** transportation

HID Ex. 2004 – Page 24
Vector Flow Inc. v. HID Global Corp.
IPR2023-00353 – Pat. No. 8,234,704

Element	Asserted Claims	References
		control systems, power supply systems, water and hydraulic control systems, warning systems, lighting systems, communications systems and miscellaneous site-specific systems such as greenhouse temperature controls." Richman at [0050] Janakiraman at [0035] Janakiraman at [0044]–[0045] "A **security system includes a central computer connected through a network to a plurality of remote computers. A database of user information is created at the central computer and copied to the remote computers. The remote computers include user interfaces for the collection of user information such a fingerprint and a user ID. When a user provides this information, the remote computer compares it to the database. If a match is generated, the remote computer authorizes access through an associated passageway.** The security system can also be used to monitor user access times and to present messages to users." Hoyos at [Abstract] "According to one aspect of the invention a security system includes a first and second unit. **The first unit generates a database of biometric features each associated with a specific person. To create this database, the first unit uses an input that generates an electronic representation of a biometric feature. The electronic representation is received by a computer processor in the first unit. This computer processor saves the first electronic representation of the biometric feature in the database of biometric features.** The second unit is coupled with the first unit by a network. The second unit is situated near an access point and is configured to control the access point based upon

HID Ex. 2004 – Page 25
Vector Flow Inc. v. HID Global Corp.
IPR2023-00353 – Pat. No. 8,234,704

Element	Asserted Claims	References
		the database of biometric features. **The access point is controlled by activating or deactivating an access device such as a locking solenoid. As with the first unit, the second unit also includes an input that generates a representation of a biometric feature. The second unit also includes a computer processor. This computer processor receives the representation of the biometric feature and compares it with the database of biometric features. If this comparison generates a match, the computer process activates (or deactivates) the access device to open the associated access point.** According to a further aspect of the invention, **the security system also includes a third unit operationally coupled with the second unit. The second and third unit are situated on opposite sides of the access point, such as a door. The third unit includes an input configured to generate an electronic representation of the biometric feature. This input is operationally coupled with the computer processor of the second unit. When this computer processor receives an electronic representation of the biometric feature from the input device of the third unit it compares it with the database of biometric features to determine whether the comparison generates a match. If so, it opens the access point.**" Hoyos at [0007] "Referring now to FIG. 1, there is shown generally a security system 10, an administration system 12, and a database integration platform 14 according to one embodiment of the present invention. **Security system 10 is an access control system such as the B.A.S.I.S.® System sold by Best Access Systems® of Indianapolis, Ind., a business unit of Stanley® Security Solutions.** As shown in FIG. 2, **security system 10 generally includes a server computing device 16, such as a workstation or personal computer, having a user interface 18, a display 20, software 22, and a security database 24 (also shown in FIG. 1), a plurality of access control panels 26 disposed at various**

HID Ex. 2004 – Page 26
Vector Flow Inc. v. HID Global Corp.
IPR2023-00353 – Pat. No. 8,234,704

Element	Asserted Claims	References
		locations throughout controlled areas of the facility, and one or more badge reader/door lock units 28 associated with each of panels 26. As is described in greater detail below, a user (e.g., a student) gains access to an area (e.g., a dorm room) by presenting his identification badge (not shown) to unit 28, which in turn verifies that the student associated with the badge has sufficient access rights (as reflected by data stored in security database 24) to enter the area, and electronically unlocks the door. An administrator of security system 10 uses computing device 16 to, among other things, assign access rights to users based on the requirements of the particular enterprise." Holloway at [0017] "**The badge data in badge ID column 81 contains the unique identification number associated with the badge in administrative system 12. The badge type field indicates that a standard badge is a subject of the data record. The badge type is essentially a template used to logically flag behavior and graphical design layout of the badge. For example, a "Staffbadgep" type may be defined, and include a blue background, allowing facility personnel to easily determine the legitimacy of the wearer's presence in a secure area. Automatic access level privileges may be assigned to a badge type as well.** Finally, a badge type also informs software 22 of security system 10 that the numbers on the badge are to be interpreted in a unique manner via card formats. A card format can dictate, for example, that the first seven digits on a magnetic stripe badge are unique to the facility, the next nine digits are the account number, and the final two digits are the issue code." Holloway at [0031] "The **present invention relates to the field of security systems, and more particularly, to a wireless security access control system**

HID Ex. 2004 – Page 27
Vector Flow Inc. v. HID Global Corp.
IPR2023-00353 – Pat. No. 8,234,704

Element	Asserted Claims	References
		controlling access to physical access points in response to access media presented by a user." Gusse at [0002] "**All access attempts are stored in the security access control device's 20 internal memory log 72. This log details the date and time along with user and access event outcome of all entry attempts made by a user**. In addition, all system events are recorded. These include, but are not limited to, logging of significant battery level changes associated with the power supply 74 (which includes a backup battery source 76), access state changes and other event invocations. At any time this audit (log) information can be down loaded to the host control station 30 via the wireless ad hoc network. **This information can also be provided in real time. In other words, the activities of any particular user is reported as status data to the host control station 30 as soon as the user tries to gain access to any physical access point 22. Similarly, any time access is attempted to any particular physical access point 22, this information is reported as status data to the host control station 30. Other real time events reported back to the host control station 30 include the status of the battery, a door is left open, etc**." Gusse at [0042] "**In addition, a weekly recurrence schedule can be configured for each entry. For example, an operator could configure a user's card 66 data to allow access to a particular group of rooms (physical access points) in a building from the beginning of January through the end of December of a given year. During this period, the operator can refine the scope of access to only allow entry on Mondays, from 1:30 pm to 3:30 pm, for example.** Customized scheduling was designed around a university environment allowing great flexibility for a large number of users, each with different access needs." Gusse at [0042]

HID Ex. 2004 – Page 28
Vector Flow Inc. v. HID Global Corp.
IPR2023-00353 – Pat. No. 8,234,704

Element	Asserted Claims	References
		Gusse at [0054] "A computer-driven resource manager (122) selectively executes user-initiated tasks (113) a**ccording to established rules (112) defining users' permissions for such tasks. A workflow engine (116) manages redefinition of the rules. Responsive to receiving (602) a request to change the rules, the engine processes the request (600). This includes reviewing the request and selecting (604) a corresponding approval path. Also, the workflow engine sequentially proceeds (610, 612, 614, 616, 620) through a sequence of stages defined by the selected path, where in each stage the workflow engine electronically solicits approvals from one or more approvers indicated by the selected approval path.** The engine continues through the stages until receiving at least one denial, or all required approvals (616). Responsive to receiving all required approvals, an electronic message is transmitted (618) directing amendment of the rules per the user request." Gill at [Abstract] "Broadly, **the ERP manager 122 monitors and selectively executes user-initiated tasks according to established rules defining users' permissions for such tasks. The rules are stored in 112, as discussed below.** In one example, the manager 122 is an enterprise software product such as SAP R/3 or mySAP from SAP, PeopleSoft or Oracle Financials from Oracle Corporation, BPCS from SSA Global Technologies, Enterprise Business System from Made2Manage Systems, NetERP from NetSuite Inc., Microsoft Dynamics from Microsoft Business Division, Ramco e.Applications from Ramco Systems, SYSPRO ERP software from SYSPRO, etc. The workflow engine 116 is a novel product that supervises redefinition of the rules 112, which is needed from time to time to accommodate hiring, firing, promotions, system reconfiguration, mergers and acquisitions, corporate reorganization, and the like." Gill at [0028]

HID Ex. 2004 – Page 29
Vector Flow Inc. v. HID Global Corp.
IPR2023-00353 – Pat. No. 8,234,704

Element	Asserted Claims	References
		"**The rules 112 indicate who can perform the tasks 113 and when. In other words, the rules 112 indicate the necessary permission that a user must have in order to cause the ERP manager 122 to perform a task 113. The engine 116 has access to the rules 112 because, as described below, the engine manages and implements changes to the rules 112.** These changes allow the ERP manager 122 to adapt as necessary to changes dictated by the organization that is operating the system 100, according to normal events such as hiring, firing, promotions, system reconfiguration, reorganizations, and the like." Gill at [0038] "**The plurality of secured Locations may be located at a single geographic site. Alternatively, or in addition, the plurality of secured Locations may be located at multiple geographic sites. The stored data may comprise data on one or more access devices, which may be tangible or intangible (keys, cards, combination codes, fingerprints, etc.) assigned to be used to provide physical entry to the Location through the entry control device. The entry control device or devices may, for example, comprise a mechanical lock, electromechanical lock, magnetic lock, or any other device designed to selectively prevent and allow physical entry to a Location.** As one of many possible examples, the entry control device may comprise a lock and the display data may comprise data on at least one of: cut keys, issued keys, or on hook keys used to open the lock." Serani at [0010] "**Device(s)" are those tangible/intangible objects, items or components of a security system which allow an authorized Device-User to gain physical access to a Location (or alternatively, deny access to an unauthorized User). Devices may be entry control devices or access devices and most security systems will need both.**

HID Ex. 2004 – Page 30
Vector Flow Inc. v. HID Global Corp.
IPR2023-00353 – Pat. No. 8,234,704

Element	Asserted Claims	References
		An example of an entry control device is a lock, while an example of an access device is a key that operates the lock. Entry control devices may comprise any other security mechanism designed to selectively allow and prevent physical access to any place. Access devices may be tangible components containing encoded criteria which are assigned to and in possession of a Device-User but are independent of the Device-User. Such access devices may be portable in that they may be moved from Device-User to Device-User or reconfigured to a different encoded criteria, such as **mechanical keys, cards such as those utilized in a card access or ATM system, Dallas Chips or other electronic signaling mechanisms, bar codes, or similar components. Access devices may be intangible components in the form of information assigned to and in possession of a Device-User, such as code number(s) utilized in keypad/combination lock processes, PIN numbers utilized in a variety of security and ATM systems, code words or phrases, or other intangible informational components used for similar purposes. Access devices may be tangible and irrevocable features of the Device-User thus performing the function of identification (encoding), such as, fingerprints, retina scans, voice patterns, and the like.** **A "Location" comprises one or more places or sites physically protected by a security mechanism or entry control device (such as one or more mechanical or electronic locks) and configured to allow physical entry by a Device-User to the place or places when the Device-User uses an appropriate access device. Locations may be diverse in that they may simply secure items (e.g., a lock box or safe of any size) or they may comprise entire buildings, areas or rooms in a building, or other physical spaces.** **"User" is an individual involved with, dependent upon, or utilizing security data composed of Devices, Locations, and Users.** **"Device-User" is one type of User which is permitted entry to defined Locations by way of the issuance and configuration of Device(s), such**

HID Ex. 2004 – Page 31
Vector Flow Inc. v. HID Global Corp.
IPR2023-00353 – Pat. No. 8,234,704

Element	Asserted Claims	References
		as an employee granted access to a department with a key, a contractor having access to a front door with a card, a driver opening a gate by way of a padlock combination, etc." Serani at [0046]
11(g)	receiving the normalized event data and applying relevant transformation and routing rules comprising condition-action sequences in order to maintain user profiles and physical security states across the plurality of sites and to resolve the actionable events through the associated specific user identities.	"**When a physical access control request event occurs, such as when a person approaches a door, one or more of the ACDs 111-116 generates an input signal to the system. For example, a reader 112 may detect an encoded user ID and transmit the credentials to DCP 117, which performs local message buffering and ACD connectivity aggregation for the door.** DCP 117 relays the ACD generated information, in the form of an access request message to the ACP 120. **ACP 120 verifies the credentials by comparing the detected credentials against the valid (authorized) credentials list and associated policies to determine if the credential is valid and if a physical access policy is associated with the credential for this ingress/egress point.** The valid credential information list and associated access policy are supplied by the physical security server 121 and is transmitted to the ACP prior to the access control event I**f the policy indicates that the door should be opened, an access control response message is transmitted from the ACP 120 to the DCP 117 to instruct it to activate (open)** the electro-mechanical lock 111 for that specific door. If the policy is to deny access because the credentials are invalid, an alarm, for example, could be triggered or sent to management station 122 and the door remains locked." Farino at [3:62] Farino Fig. 9

HID Ex. 2004 – Page 32
Vector Flow Inc. v. HID Global Corp.
IPR2023-00353 – Pat. No. 8,234,704

Element	Asserted Claims	References
		"The **EMP further includes a Decider Module having a set of rules which have been predefined by the Administrative user.** The Decider Module includes an inference engine which is capable of recording the history of previous event management records to thereby determine how to respond to in-coming event data. As the **Decider Module monitors and reads the in-coming event data, it analyses the event data, against the Rule Base and when necessary the Decider Module passes the event data to an Alert Handler Module (AHM) which determines an appropriate action.** For example, the alert handler may decide to notify the Administrative user that a particular event has occurred." Sweeney at [6:04] "8. Decryption Module 216. **This module decodes an XML based SCA coded message back into standardized XML format. Thus, the input for this module is an encrypted message, and the output is a standardized message in XML format with an appended data integrity control element.**" Richman at [0104] Farino at [16:36] "A unified policy engine 410, which is a part of unified access control server 400, acts as the point of unification for lists and policies that tie physical access policies and events to network policies and events. Unified policy engine 410 and unified access control server 400 may also provide pre-defined default policies when physical access lists or policies do not logically agree with network access control lists and policies. Engine 400 generates and transmits policy-based instructions to physical security system 200 as well as frame/packet network 204 in response to an event or combination of events to facility access or network connected devices such that the access control and network

HID Ex. 2004 – Page 33
Vector Flow Inc. v. HID Global Corp.
IPR2023-00353 – Pat. No. 8,234,704

Element	Asserted Claims	References
		connected devices perform the specified action. Engine 400 logs all attempts to access a physical facility or a network resource and implements policy-based instructions in response to each or any access attempt. Engine 400 may communicate with a separate management station for monitoring network resources and access control events throughout the system, even if the system spans multiple facilities and multiple networks." Farino at [17:30] Janakiraman at [0044]–[0045]
Claim 12		
12	The method of claim 11 wherein the plurality of sensor types comprise physical access, intrusion, and environmental conditions, and wherein the action events comprise at least one of generating an audible alarm, notifying authority personnel, initiating lockdown mode of the site, initiating computer backup and shutdown procedures, and facilitating exit from the site.	See claim 11 above. "With reference now to FIG. 3, a block diagram depicts a portion of a physical building that employs a prior art personal physical proximity detector system to control various electrical devices within the building. **Building 300 contains multiple offices, hallways, and other physical spaces. Hallway 302 contains electronic physical proximity devices 304 and 306, and offices 308 and 310 contain electronic physical proximity detecting devices 312 and 314, respectively, as well as computers 316 and 318, respectively.** Person 320 wears or carries electronic physical proximity device 322, e.g., in the form of an electronic security badge, PDA, cell phone, or other computational device." Janakiraman at [0037] Janakiraman at [0045] "**An asset protection system and method integrates physical asset security with information asset security in a hosted environment**, or

HID Ex. 2004 – Page 34
Vector Flow Inc. v. HID Global Corp.
IPR2023-00353 – Pat. No. 8,234,704

Element	Asserted Claims	References
		in certain circumstances in a users environment, as a security application service provider (SASP). The SASP allows customers to acquire computer-based applications for use in information security and/or asset protection, and have those applications developed, integrated, maintained and/or operated, all in a single location. **The hosted environment provides security access, generates reports, triggers alerts, and performs analysis based on usage patterns.** Usage patterns of repeat system users are learned, such that an anomalous usage results in corrective action, and include physical entry data, logon and logoff times for various equipment, usage periods and file access for various information technology applications, and ingress/egress operation patterns as viewed from a monitoring device. Additionally, a visitor tracking system permits access to registered visitors having authorization. The registered visitors are authenticated using biometrics." Flemming at [Abstract] "**If a user attempts to gain physical access to a door without valid credentials, then the denied entry attempt is logged in** the physical access database and **reflected in the gatekeeper log files to trigger alarms and/or for later use in forensic study and predictive modeling.** Detection and reaction is based on a set of rules consistent with the client's needs and threat levels." Flemming at [0053] Flemming at [0054] "In a different or additional embodiment, **the resource 115 may include data, processes, computing hardware, electronics, devices, or actions relating to building security or so-called "physical provisioning."** In this embodiment, **the resource 115 includes various remotely operated facility security components such as door locks, alarm systems, access zones, controllers, boom gates, elevators, HVAC systems and**

HID Ex. 2004 – Page 35
Vector Flow Inc. v. HID Global Corp.
IPR2023-00353 – Pat. No. 8,234,704

Element	Asserted Claims	References
		components, readers (card, biometric, RFID etc), Positive ID Readers (PIRs) and the events and alarms that are generated by these components. It can also be extended to include other devices such as photocopiers, POS systems, transportation access (charge) points and other such systems that can be incorporated on smart card or other physical access technology." Gill at [0105] "In the **physical provisioning context, the tasks 113 include acts of opening the door locks, deactivating the alarm systems, granting and revoking access to physical areas, and the like**. In processing these tasks, the ERP manager **122** receives and evaluates individual user authentication from interfaces such as **118**, **120**. User authentication may utilize keypad passcode, biometric identification (e.g., fingerprint, iris/retina scan), user name and password submittal, presentation of magnetic stripe card, proximity card, smart card, use of a radio frequency identification (RFID), etc. The ERP manager **122** considers information such as the user's role and other characteristics (from **112**, **114**) to determine whether to perform the requested task (**113**) on behalf of the user." Gill at [0106] "In another aspect of the invention, **an interactive system for security management is accessible via a communications network by a plurality of DB-Users is adapted to manage a security system associated with places physically protected by corresponding security components used to control physical entry to the places.** The system comprises at least one searchable database having stored data associated with securing the places via the security components. Software may be configured to allow a DB-User to search the stored data in the database and to display a set of data based on the stored data. The Software may also be configured to allow the DB-User to compare

HID Ex. 2004 – Page 36
Vector Flow Inc. v. HID Global Corp.
IPR2023-00353 – Pat. No. 8,234,704

Element	Asserted Claims	References
		the displayed data to actual data obtained at one of the places for audit purposes." Serani at [0014] "At **least one of the security access control devices transmits status data to the host control system via the wireless ad hoc network.** The status data may comprise at least one of battery status, user status, and security access control device operating status. The status data may be transmitted in real time. **The security access control device operating status may comprise at least one of an unlocked state, a card controlled state, an access disabled state, and a dual mode state.** In addition, the status **data may comprise audit data, wherein the audit data includes system events, access attempts by a user, and a time and access event outcome of the access attempts made by the user**." Gusse at [0013] "Referring initially to FIG. 1, **a security access control system 10 comprises a plurality of security access control devices 20(1)-20(*n*) at respective physical access points 22(1)-22(*n*) for controlling physical access thereat.** A physical access point **22**(**1**)-**22**(*n*) may be any area in which entry by a user needs to be controlled and monitored. For instance, the physical access points **22**(**1**)-**22**(*n*) at a university are staff offices, professor offices, lab rooms, supply rooms, etc. These are fixed physical access points." Gusse at [0022] "The access **media reader 64 is used when a user inserts a card 66 to try to gain entry to a door at the physical access point 26.** When the **card 66 is inserted the card reader 64 initiates communication with the access media (i.e., the card 66) and issues a decryption key. It is then able to check the access media 66 to determine if that user has access to that room.** The access attempt is then logged in memory **72**.

HID Ex. 2004 – Page 37
Vector Flow Inc. v. HID Global Corp.
IPR2023-00353 – Pat. No. 8,234,704

Element	Asserted Claims	References
		The main microcontroller **26** includes a processor **70** for handling all of the above-mentioned tasks. In lieu of a processor, a programmable gate array may be used, as readily appreciated by those skilled in the art. The main microcontroller **26** also coordinates communication with the transceiver **24** and controls the access media reader **64**, event schedules with the real time clock **62**, user validation, and motor controls **60**." Gusse at [0033] "A **system for controlling access to a building or facility having portals (e.g., doors, garages, walkways, windows, etc.) that are opened or closed by locks based on identity information detected by identity information detection means (e.g., access card readers, keypads, touch screens, biometric devices such as fingerprint readers, eye-scan (e.g., retina scan) detectors, voice recognition detectors, etc.).** The system comprises a server interfaced with the identity information detection means and with locks on the portals and wherein access through the portals is modified by government-issued threat levels (e.g., Department of Homeland Security Levels 1-5)." Monaco at [01:52] "FIG. 1 depicts **an access network 100 used to verify the identity of at least one credential, usually an RFID credential.** In one embodiment of the present invention, the system **100 comprises a control panel 104, a plurality of reader/writers 108 *a*-K, where K is an integer and is typically greater than or equal to one, and one or more credentials 120.** The plurality **of reader/writers 108 *a*-K may include reader/writers 108 of the same type, as well as reader/writers of different types.** For example, a subset of the plurality of reader/writers **108** *a*-K may be RF enabled and are capable of communicating with credentials **120**. Whereas another subset of the plurality of reader/writers **108** *a*-K may employ other machine

HID Ex. 2004 – Page 38
Vector Flow Inc. v. HID Global Corp.
IPR2023-00353 – Pat. No. 8,234,704

Element	Asserted Claims	References
		reading/writing non-RF machine reading modalities such as magnets, lights, infrared, and so on." Davis at [0028] "**One function of a reader/writer 108 is to control access to certain assets.** More specifically, a **reader/writer 108 may be positioned at an access point for a given asset** (e.g., a door for a room, building, or safe, a computer for electronic files, and so on). Unless a proper credential **120** is presented to the reader/writer **108**, the access point is maintained in a secure state such that admittance or access to the asset is denied. **If a credential 120 having authority to access the asset is presented to the reader/writer 108, then the reader/writer 108 has the discretion to allow the user of the credential 120 access to the asset** and implement various actions accordingly." Davis at [0030] "Step 385 occurs when the user requests access to the network at given a network port (e.g. a specific port connection on a specific network infrastructure device such as a switch located in the same general physical areas as the physical ACD used in steps 381 through 384). This initial log in request is sent to the unified access control server 200. Server 200 executes the associated access control policy for the computer based on verification of the credentials. More specifically, server 200 verifies that the user is authorized to access the network from the present location. If the user is not authorized to be in a facility or is not authorized to access certain computer resources at a specific facility, access may be denied and an alarm or alert may be issued to security personnel. If the policy is to allow access, the user is granted access to the networked computer resources. Then, server 200 may request the network infrastructure device (such as a switch) to download the network policy for this computer as indicated at step 386. Hence, the

HID Ex. 2004 – Page 39
Vector Flow Inc. v. HID Global Corp.
IPR2023-00353 – Pat. No. 8,234,704

Element	Asserted Claims	References
		present invention enables correlation of events in the physical realm with events occurring on corporate network resources and vice versa." Farino at [16:63] Farino at [11:11] "Yet another object of the instant invention is to provide a computer implemented communications protocol whereby bi-directional data and command transmissions may occur between a base station and any designated personal identification devices, which enables assistance deployment and transmits the location of the person, group of persons, security guards and/or guard vehicles." Richman at [0053] "A schematic diagram of checkpoint computer communications options 70 is illustrated in FIG. 4. Another embodiment of a checkpoint computer 72 receives and records information from peripheral event sensor equipment. Most of these devices, such as an access control system 94 coupled with a motion detection device 74, an identification or ID tracking device 76, an GPS tracking system or tracking device 78, a temperature sensor 96 coupled with a fire and smoke detection device 82, perimeter control systems 98, a hand held device 84 such as various security guard communications equipment or a PDA-type device, video camera subsystems 86, climate control subsystems 88 such as heating ventilating and air conditioning (HVAC) subsystems, and transport subsystems 92 such as elevator control device, will all send information instantly and simultaneously to the checkpoint computer 72 by means of a security system communications protocol through an embedded Input/Output (I/0) microprocessor, as shown within the checkpoint computer 72." Richman at [0084]

HID Ex. 2004 – Page 40
Vector Flow Inc. v. HID Global Corp.
IPR2023-00353 – Pat. No. 8,234,704

Element	Asserted Claims	References
		Hoyos at [0041]–[0043] Ahmed at Abstract "Most commercial properties include a number of building systems that monitor and regulate various functions of the building for the comfort and well-being of the tenants. These building systems include security systems, fire control systems, and elevator systems. One prevalent and important building system is the environmental control system. An environmental control system is used to regulate the temperature and flow of air throughout a building." Ahmed at [0004]–[0005]
Claim 13		
13	The method of claim 11 further comprising converting the native data representation format for each security sensor into XML (Extensible Markup Language) format, and wherein the native data representation format encompasses native sensor data including text data and binary data represented in a proprietary format, and wherein the native sensor data includes at least one of a command or sensor state information.	See claim 11 above. "Therefore, a new and improved computer implemented communications protocol is provided, which is an **XML based communications protocol for security monitoring purposes.** T**his unique XML based communications protocol is implemented through numerous modules which receive and convert data messages from diverse security devices and sensors, standardize and send converted messages, and encrypt and decrypt said data messages as necessary.** With the set modules, the data messages are filtered and transmitted from checkpoint computers to base station computers, which analyzes, reports and logs environmental as well as security events within a subject site. The resulting integrated security system provides better trained security guards, who are more alert and responsive, and more closely supervised and easily scheduled, enhanced financial monitoring, more accurately paid and costed security services, better archived and reported security related events, as well as being better coordinated with public agencies,

HID Ex. 2004 – Page 41
Vector Flow Inc. v. HID Global Corp.
IPR2023-00353 – Pat. No. 8,234,704

Element	Asserted Claims	References
		enhanced safety, and readily upgraded and integrated with existing and future technologies." Richman at [0066] "Site specific communication protocols, to collect data from sensors, will be developed and deployed for each project. The universal communications protocol, comprised of an encrypted XML-enabled proprietary software program, will direct communications between the checkpoint data processing subsystems or checkpoint computers and the base stations as well as any headquarters servers deployed within the system (see FIG. 5 and FIG. 6 below). FIG. 5 is a block diagram of a checkpoint computer hardware architecture in greater detail 100. The CPU microprocessor controller 102 converts the incoming and outgoing signals by means of application software which is stored in the memory (ROM and RAM) 104 of the checkpoint." Richman at [0085]–[0086] "Turning now to FIG. 6, there is illustrated a block diagram of an integrated security system encrypted XML communications protocol 120 exemplifying communications between checkpoints and the system core application at a base station, as constructed in accordance with the present invention. The system sensors 122 communicate any (and all) system event 124 to a checkpoint 130 via a custom protocol." Richman at [0086] "The attribute code(s) and value(s) 136, together with associated sensor code 132 and event code 134 for a given system event 124, are detected and processed by the checkpoint encrypted XML communications protocol software which generates the encrypted XML message which can then be transferred over the network, LAN or a global computer network such as the Internet."

HID Ex. 2004 – Page 42
Vector Flow Inc. v. HID Global Corp.
IPR2023-00353 – Pat. No. 8,234,704

Element	Asserted Claims	References
		Richman at [0089] "Referring now to FIG. 7, in operation, under Level I 190, security devices and sensors transmit data in device language specific for that device or sensor. Under Level II 192 a checkpoint data processing unit collects data messages from various site security devices and sensors in unique device language and translates these messages into standardized messages to be passed on to the SCA. This is accomplished by generating a message based upon converted coded data messages and transmitting the converted messages to computers containing the SCA. Under Level III 196, base station computers and/or off site headquarters computers, or any other off site computers (such as remote workstations), analyze the coded transmitted messages whereby such analysis is used to generate reports and logs for the purpose of effectively monitoring the environmental and security conditions within a subject site." Richman at [0092]–[0093] "Therefore, Level I 190 operations include data transmission from any number of existing, or yet to be created, security devices and event sensors, either off the shelf units and/or customized combinations, all having their own specialized and unique device language transmitting components and qualities. In this regard, the present invention can be programmed to receive all of the data message formats originating from any and all of these devices, then be integrated into any site for security and/or environmental monitoring in a customized and readily scalable fashion." Richman at [0094] "1. Conversion Module 202. **This module receives data from security hardware devices of varying types in their own specialized unique data format and converts this data into a standardized XML formatted message.** Each unique hardware device requires a separate

HID Ex. 2004 – Page 43
Vector Flow Inc. v. HID Global Corp.
IPR2023-00353 – Pat. No. 8,234,704

Element	Asserted Claims	References
		customized conversion module to translate its data into the coded SCA XML format for the purpose of further analysis. Thus, for this module, the input is a varying hardware signal, and the output is a standardized message in XML format." Richman at [0097] "**Sensor code: The sensor code is the identification of the sensor/device that produces a particular event.** **Event code: The event code is the identification of the actual event that happened. The event code, together with the sensor code is unique and will be logged in the event log.** **Attribute code: The attribute codes are attributes of the event code and describe values for the event. Each event can have several attributes. The value of an attribute could be anything from an integer to a string to an image or other data.**" Richman at [0111] "**The generated code by the checkpoint could be encrypted (see security protocol) in order to keep the information undisclosed while it is transferred over the network or internet.** After these 3 elements have been received by the BS, the SCA will process and decrypt the incoming XML code. **The "event code" and "sensor code" will generate an entry in the event log. An SQL trigger or stored procedure will process the attributes of the event. They will compare the attribute values to the alarm values stored in the database and generate an alarm event accordingly. The alarm event is stored in the alarm log.**" Richman at [0115] "An embodiment of the system of the **present invention may also include a data collector interface for coupling external data sources**

HID Ex. 2004 – Page 44
Vector Flow Inc. v. HID Global Corp.
IPR2023-00353 – Pat. No. 8,234,704

Element	Asserted Claims	References
		to the database. The **data collector interface converts data from the native format for an external data source to one that is compatible with the structure of the database in which the data is stored**. This data conversion function of the data collector interface enables the database or databases of the present invention to be coupled to a plurality of external data sources without requiring that all of the external data sources conform to one particular database structure. Furthermore, the data collector interface includes transaction services that generate the instructions for a database API that are required to store the data in the database. **Thus, data sources from diverse locations may be coupled to a database at a common site**. Consequently, a significant accumulation of historical data may be obtained for a data mart component of the database, which further enhances the value of the data mining applications at the common site. However, the data provider interface also supports the segregation of the collected data into different databases so control application programs may be developed from the data originated at the particular building site for which the application is being developed." Ahmed at [0029] "Data collector services 114, FIG. 2A, include activities that may be activated by scheduling services 110 for the purpose of providing data from an external data source 120 in a common data format to a transaction service 118 (FIG. 3). Preferably, the native format data of external data sources 120 are converted to an XML schema, although common data representation schema may be used. Transaction service 118 reads the collected data and uses it to populate the data structures of database 18." Ahmed at [0072]

HID Ex. 2004 – Page 45
Vector Flow Inc. v. HID Global Corp.
IPR2023-00353 – Pat. No. 8,234,704

Element	Asserted Claims	References
		"The audit servers 12 are preferably strategically deployed around the global network to gather facts about wired 16 or wireless 22 local networks within the global network. According to one embodiment of the invention, **the audit servers 12 are configured to gather facts relating to the wired and/or wireless 22 local networks using heterogeneous information sources. Such information sources may include scanners, cameras, manually entered data, and/or the like. The data gathered by each information source is converted into a normalized data format, such as, for example, and XML (Extensible Markup Language), and stored in the audit repository 14 for access by the compliance server 10.**" Williams at [04:65] "According to one embodiment of the invention, the scan harness 212 works with one or more scanners 204-210 to launch a pre-configured audit based on the target list created by the topology analytic engine 200 at a pre-determined time as scheduled by the compliance server 10. In this regard, the scan harness 212 provides necessary input to the various heterogeneous scanners 204-210, and receives the scan results that represent the facts gathered about the network as output. **The scan results are often heterogeneous in their format when heterogeneous scanners are used. The scan harness 212 takes the scan results in their heterogeneous formats, and automatically converts them into a single, normalized data format. According to one embodiment of the invention, the normalized data format is a machine-processable language format such as XML, which, according to one embodiment of the invention, is normalized for structure but not for semantic equivalence. According to this embodiment, semantic equivalence normalization is done in the P&V engine 34 (FIG. 2) as is described in further detail below. In making the automatic conversion of the data format structure, the scan harness 212 may utilize a conversion table that maps known fields in the output of a particular scanner**

HID Ex. 2004 – Page 46
Vector Flow Inc. v. HID Global Corp.
IPR2023-00353 – Pat. No. 8,234,704

Element	Asserted Claims	References
		into XML fields used in the XML format. The normalization allows the scan results to be consistently parsed and stored in the audit repository 14." Williams at [11:57] "Regardless of a method in which the network information is obtained, **each audit server 12 generates a scan results document 220 with scan data that is normalized into a standard XML format. The P&V engine 34 (FIG. 2) resident in the compliance server 10 then applies one or more policies to the scan results.** According to one embodiment of the invention, the pattern matching and transformation aspects of the P&V engine 34 are implemented via an XLST processor conventional in the art." Williams at [15:06]
Claim 14		
14	The method of claim 11 further comprising applying, through a rules engine, defined rules on the data and commands from each security sensor, wherein each rule has an associated action and one rule is applied at a time to the normalized event data in a sequential order dictated by one of a defined rule execution order or a top to bottom order based on event time.	See claim 11 above. "The EMP further includes a Decider Module having a set of rules which have been predefined by the Administrative user. The Decider Module includes an inference engine which is capable of recording the history of previous event management records to thereby determine how to respond to in-coming event data. As the Decider Module monitors and reads the in-coming event data, it analyses the event data, against the Rule Base and when necessary the Decider Module passes the event data to an Alert Handler Module (AHM) which determines an appropriate action. For example, the alert handler may decide to notify the Administrative user that a particular event has occurred. The Rule Base can be amended by a Rule Interpreter Module (RIM) also included in the EMP so as to enable a user to amend the rules base

HID Ex. 2004 – Page 47
Vector Flow Inc. v. HID Global Corp.
IPR2023-00353 – Pat. No. 8,234,704

Element	Asserted Claims	References
		and thereby customise the response of the event manager program for the Administrative user's needs." Sweeney at [6:4]
Claim 15		
15	The method of claim 11 further comprising representing, through a visual editor, each normalized physical sensor as an object containing one or more attributes that define a spatial relationship to other objects through one or more defined rules, the visual editor including a drag and drop graphical user interface component that facilitates creation of rules through interconnection of rule objects and definition of rule properties.	See claim 11 above.

HID Ex. 2004 – Page 48
Vector Flow Inc. v. HID Global Corp.
IPR2023-00353 – Pat. No. 8,234,704