

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE**

HID GLOBAL CORPORATION,

Plaintiff,

v.

VECTOR FLOW, INC. et al.,

Defendant.

**Civil Action No. 21-1769 (GBW)
(CONSOLIDATED)**

**DECLARATION OF MARK JONES IN SUPPORT OF PLAINTIFF
HID GLOBAL CORPORATION'S OPENING CLAIM CONSTRUCTION BRIEF**

I, Mark Jones, do hereby declare as follows:

1. INTRODUCTION

1. I have been retained by counsel for HID Global Corporation ("HID"), as an expert in the lawsuit captioned above.

2. I have reviewed U.S. Patent No. 8,234,704 (the "'704 Patent") (Ex. 1) and U.S. Patent No. 9,111,088 (the "'088 Patent") (Ex. 2) (collectively, the "Asserted Patents"), the prosecution file histories for the Asserted Patents, the parties' Joint Claim Construction Chart and exhibits to the same, and the exhibits cited in this declaration. In reaching the opinions expressed in this declaration, I have also relied on years of education, teaching, research, and experience, and my understanding of the applicable legal principles.

3. This declaration represents those opinions I have formed to date, and I reserve the right to revise, supplement, and amend the opinions stated herein based on new information and on my continuing analysis of the materials already considered.

2. QUALIFICATIONS

4. I am a Professor Emeritus of Electrical and Computer Engineering at Virginia Tech in Blacksburg, Virginia. I graduated summa cum laude from Clemson University in 1986 with a B.S. in Computer Science and a minor in Computer Engineering, while holding a National Merit Scholarship and the R. F. Poole Scholarship. I then graduated from Duke University in 1990 with a PhD in Computer Science, while holding the Von Neumann Fellowship.

5. Upon graduation, I joined the Department of Energy at its Argonne National Laboratory facility. My responsibilities there included the design and use of software for computers with hundreds of processing elements. This software was designed for compatibility with new parallel computer architectures as they became available, as well as with other large software components being written in the Department of Energy. While with the Department of Energy, I received the IEEE Gordon Bell Prize.

6. In 1994, I joined the Computer Science faculty at the University of Tennessee. My teaching responsibilities included computer architecture and computer networking. My research interests included the design and use of software that used the collective power of large groups of workstations. While at the University of Tennessee, I received a CAREER Award from the National Science Foundation.

7. In 1997, I joined the Electrical and Computer Engineering faculty at Virginia Tech. My teaching responsibilities have included the design of embedded systems, computer organization, computer architecture, a variety of programming courses, and parallel computing. I have been cited multiple times on the College of Engineering's Dean's List for teaching.

8. In addition to the activities, education, and professional experience listed above, I have been involved in research projects that contribute to my expertise relating to this declaration.

While at Virginia Tech, I have been a primary or co-investigator on government and industrial research grants and contracts in excess of five million dollars.

9. The majority of the research contracts undertaken in the laboratory have involved collaboration and coordination with other groups to build a larger system. My responsibilities under the SLAAC project (a collaborative effort funded by the Defense Advanced Research Projects Agency involving the University of Southern California, Sandia National Laboratory, Los Alamos National Laboratory, Brigham Young University, UCLA, Lockheed-Martin, and the United States Navy) included the development of a software system for monitoring, configuring, and controlling a networked collection of computers hosting specialized computer hardware. As part of the DSN project (a collaborative effort funded by the Defense Advanced Research Projects Agency involving UCLA and USC), I was responsible for designing algorithms and software for controlling and monitoring a large network of autonomous computer sensor nodes. This software was integrated with software from several other teams around the country for a set of field demonstrations over a three-year period.

10. In the TEAMDEC project for the Air Force Research Laboratory, I led an effort to design and construct a collaborative, Internet-based decision-making system. This Java-based system provided a geographically diverse team with Internet-based tools to enable collaborative decision-making. On the server side, the system architecture made extensive use of database technology. This work was awarded first prize at the 2002 AOL/CIT Research Day.

11. Other projects have involved the close coupling of computer hardware and software, including the writing of device drivers and simple operating systems, the design of hardware circuits, the design of new system architectures, architectures for secure computing, the

modification of complex operating systems, and software for mediating between complex software packages.

12. A detailed record of my professional qualifications is set forth in the attached Exhibit 4, which is my curriculum vitae, including a list of publications, awards, research grants, and professional activities. My curriculum vitae also lists the depositions, hearings, and trials at which I have testified. I am being compensated at the rate of \$650 per hour for my work in connection with this case. My compensation is in no way related to the outcome of this litigation. If called as a witness, I would testify as to the statements and opinions contained in this declaration.

3. LEGAL UNDERSTANDING

13. I am not a legal expert and offer no legal opinions. I have been advised of the following general principles of patent law to be considered in formulating my opinions. I have applied these principles to the facts set forth in this declaration in rendering my opinions.

3.1. Claim Construction

14. I understand that the claims of a patent define the scope of the invention and the patentee's rights. I further understand that claim construction is a matter of law and that claims are to be construed by the Court.

15. I understand that, as a default rule, courts are to construe claims in accordance with the plain and ordinary meaning they would have to one of ordinary skill in the art in light of the claim language, specification, and prosecution history (*i.e.*, the intrinsic record). In this regard, I understand that courts determine the proper meaning of a disputed claim term by first looking to the claim language itself, and then to the remaining intrinsic record, but that courts should not import limitations into the claims. I further understand that extrinsic evidence outside the intrinsic record—such as treatises and dictionaries—may also be considered as an aid in arriving at the proper construction.

16. I understand that there are only two circumstances in which a court may depart from the plain and ordinary meaning: 1) when a patentee sets out a definition and acts as its own lexicographer, or 2) when the patentee disavows the full scope of a claim term either in the specification or during prosecution. I understand that the standards for lexicography and disavowal are often described as “exacting,” and that lexicography generally requires that a patentee must clearly set forth a definition of the disputed claim term other than its plain and ordinary meaning and must clearly express an intent to redefine the term. Similarly, disavowal generally requires that the specification or prosecution history make clear that the invention does not include a particular feature, or is clearly limited to a particular form of the invention..

3.2. Indefiniteness

17. I understand that patent claims are presumed valid, and that the patent challenger bears the burden of establishing invalidity by clear and convincing evidence. I understand that the Patent Act requires patent claims to particularly point out and distinctly claim the subject matter that the applicant regards as the invention. I understand that a claim is said to be “indefinite” only if, when viewed in light of the intrinsic record, it fails to inform those skilled in the art about the scope of the invention with reasonable certainty.

18. I understand that Section 112(f) of the Patent Act permits a claim to be expressed as a means or step for performing a specified function without the recital of structure, material, or acts in support thereof. I understand that the use of the word “means” in a claim element creates a rebuttable presumption that 35 U.S.C. § 112(f) applies. In addition, I understand that generic terms—such as “mechanism,” “element,” “device,” and other so-called “nonce” words—that reflect nothing more than verbal constructs may be used in a claim in a manner that is tantamount to using the word “means” if they do not connote sufficiently definite structure.

19. I understand that construction of a means-plus-function term is a two-step process. First, the court identifies the claimed function. Second, the court determines the structure disclosed in the specification that corresponds to the claimed function. The structure disclosed in the specification only qualifies as “corresponding structure” if the intrinsic evidence clearly associates that structure to the function recited in the claim.

20. I understand a patent may be invalid for indefiniteness if it invokes Section 112(f) but the specification fails disclose any “corresponding structure” for performing the claimed function.

4. THE ASSERTED PATENTS

21. HID asserts the following claims against Defendants (“Vector Flow”): method claims 11-15 of the ’704 Patent; and method claims 15-17, 19, and 20 of the ’088 Patent (collectively, the “Asserted Claims”).

22. The Asserted Patents contain a substantial amount of overlapping disclosure. They both “relate generally to physical security systems, and more specifically to a system for integrating disparate security systems using a rules-based policy engine and normalized data format.” ’704 Patent at 1:24-27; ’088 Patent at 1:23-26. Both patents further explain that “[m]any different physical security systems are available on the market, and are manufactured by a variety of vendors, each of which may have its own standards of data representation and exchange.” ’704 Patent at 1:53-56; ’088 Patent at 1:51-54. As such, these systems “can have multiple representations of individuals or assets, and non-uniform policies for access to physical resources.” ’704 Patent at 1:59-65; ’088 Patent at 1:57-63. Because “[t]he access and alarm events from different physical security systems generally do not follow standard definitions,” “[t]his prevents the creation of uniform policy, enforcement and compliance procedures across corporations and multiple systems.” ’704 Patent at 1:65-2:2; ’088 Patent at 1:63-67.

23. The Asserted Patents each solve this problem using slightly different solutions. The '704 Patent's solution is directed to: "defining a uniform data format for entities and events controlled by disparate physical security systems," "defining ... physical security policies and enforc[ing] them on disparate security systems, data changes and events," and "translat[ing] the [] policies to [a] standardized rules format that can be enforced in real-time by a policy engine." '704 Patent at 2:11-23. The '088 Patent's solution is directed to: "integrating and normalizing physical security data, states and events from disparate physical security systems, devices and sensors to maintain in real-time rules based policy state information to enforce physical security policies uniformly across network and information technology (IT) systems." '088 Patent at 2:26-53. Further distinctions between the Asserted Patents can be found in the Asserted Claims.

5. LEVEL OF ORDINARY SKILL IN THE ART

24. It is my understanding that I must address the issues set forth in this declaration from the viewpoint of a person of ordinary skill in the art ("POSITA") at the time of the invention to which the Asserted Patents pertain, which I have been informed, is August 14, 2006.

25. I understand that a POSITA is a person who is trained in the relevant technical field of a patent without possessing extraordinary or otherwise exceptional skill. I further understand that factors such as the education level of those working in the field, the sophistication of the technology, the types of problems encountered in the art, prior art solutions to those problems, and the speed at which innovations are made, may help establish the level of ordinary skill in the art.

26. Taking these factors into consideration, it is my opinion that a POSITA at the time of the Asserted Patents' inventions would have been an individual who has completed a Bachelor of Science degree in Computer Science, or equivalent field, and had approximately three years of professional experience in the design or development of distributed computer systems (although,

for example, more professional experience may compensate for less formal education, and vice versa).

27. I myself, based on my education and experience as described above, both met and exceeded the qualifications and background of a POSITA.

6. TERMS IN DISPUTE

28. I have been asked to provide my opinions on the terms addressed below.

6.1. Term 1: “sensor” (’704 Patent, cls. 11-15; ’088 Patent, cl. 15)

HID’s Proposed Construction	Vector Flow’s Proposed Construction
No construction necessary; Plain and ordinary meaning	“a device that responds to a physical stimulus and transmits a resulting signal”

6.2. Term 2: “sensor data” (’704 Patent, cls. 11, 13)

HID’s Proposed Construction	Vector Flow’s Proposed Construction
No construction necessary; Plain and ordinary meaning	“the data transmitted by a sensor in response to a physical stimulus”

29. In my opinion, Terms 1 and 2 should be construed in accordance with their plain and ordinary meanings.

30. I have reviewed the claims’ various uses of “sensor” and “sensor data,” and in my opinion, the claims use these words in accord with their plain and ordinary meaning, which is readily understood by a POSITA. In particular, a POSITA reading the claims in the context of the specification would understand that a “sensor” is a device configured to detect information, and that “sensor data” is data associated with a sensor. This understanding is consistent with the claim language, which, as shown below, already defines many aspects of the sensor’s operation:

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;
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;

'704 Patent at cl. 11.

31. Similarly, the specifications of both Asserted Patents repeatedly use Terms 1 and 2 consistently with their plain and ordinary meaning, which, as discussed above, is consistent with the claim language. For example, three passages from the Asserted Patents are shown below:

cal security systems. Thus, as shown in FIG. 1A, facility **102** contains a physical security system **102** that controls security elements, such as access control, alarms **105**, and monitors and sensors **107**. Facility **102** may represent a house or office building, or any other type of structure that contains some level of physical security infrastructure. The alarm and monitor elements of the physical security systems represent various access control, monitoring, surveillance, sensor, or other asset protection mechanisms that may be employed throughout the facility. These can be independent elements that are

'704 Patent at 4:6-15.

cal security systems. Thus, as shown in FIG. 1A, facility **102** contains a physical security system **103** that controls security elements, such as alarms **105**, and monitors and sensors **107**. Facility **102** may represent a house or office building, or any other type of structure that contains some level of physical security infrastructure. The alarm and monitor elements of the physical security systems represent various access control, monitoring, surveillance, sensor, or other asset protection mechanisms that may be employed throughout the facility. These can be independent elements that are configured to

'088 Patent at 4:25-34.

504. The system collects data and alarm events from physical sensors, monitors and/or alarms distributed throughout the monitored facilities, such as facilities **102** and **103** in FIG. 1A, block **506**. This data is collected in native format and then

'704 Patent at 11:63-66; '088 Patent at 13:28-31.

32. As shown above, the '704 Patent describes sensors as devices that are configured to detect information within the security system. They are **not**, as Vector Flow asserts, limited to only sensors that “respond[] to a physical stimulus and transmit[] a resulting signal.”

33. These descriptions from the intrinsic record are further consistent with the extrinsic evidence. For example, the term “sensor” appears in a technical dictionary:

the use of **sensitometers**.
sensor **1.** A component, circuit, device, instrument, piece of equipment, system, material, or mechanism which serves to **sense (1)**, and respond. A sensor may, for instance, detect a given value, or any change in values. There are many examples, including acoustic, pressure, contact, force, motion, proximity, position, light, optical, radiation, infrared, ultraviolet, radio-frequency, magnetic, photoelectric, and time sensors. Most sensors convert a non-electrical phenomenon into a proportional electrical equivalent, and nearly all transducers are sensors of some kind. A sensor may provide an analog or digital output, the latter being used, for instance, for computer applications. Contact sensors detect objects and phenomena through physical contact with an object or medium, while non-contact sensors have no such contact. **2.** Same as **sensing element**.

Ex. 9 (Wiley Electrical & Electronics Engineering Dictionary) (2004).

34. From the above evidence, and based on my review of the Asserted Patents, it is clear the terms “sensor” and “sensor data” are used by the Asserted Patents in accord with their plain and ordinary meaning, and are well understood by a POSITA upon reading the claims in light of the specification.

35. In my opinion, Vector Flow’s proposed construction is incorrect because it is too narrow. For example, not all sensors always “respond[] to a physical stimulus” and always “transmit[] a resulting signal.” As the dictionary definition above makes clear, some sensors may just detect or collect “sensor data” and need not necessarily transmit a resulting signal. Indeed, the Asserted Patents describe using sensors to collect data. *See, e.g.*, ’704 Patent, 11:63-65 (“The system collects data and alarm events from physical sensors, monitors and/or alarms distributed throughout the monitored facilities...”); ’088 Patent, 13:28-30 (same). Additionally, sensors can respond to non-physical stimuli, such as the time sensor example identified in the above dictionary definition, or sensors that are triggered based on the execution of software routines, such as the “IT intrusion” and “computer hacking” events described by the Asserted Patents. *See, e.g.*, ’704 Patent, 4:15-18, 12:19-25; ’088 Patent, 4:34-37, 13:51-57. Moreover, Vector Flow’s proposed construction is too narrow because the sensor data includes more than “data transmitted by a sensor in response to a physical stimulus.” For example, dependent claim 13 of the ’704 Patent recites that the “sensor data” includes “text data and binary data represented in a proprietary format,” as well as “a command or sensor state information.” Vector Flow’s proposed construction seemingly excludes these embodiments.

36. In addition, Vector Flow’s construction would lead to confusion because it cannot coherently be inserted into the Asserted Claims. The Asserted Claims use the terms “sensor” and “sensor data” in various contexts and formats. For example, claim 11 of the ’704 Patent recites the steps of “interfacing ... a plurality of **security sensor types**” and “accepting **sensor data** from each **security sensor** an integration module.”¹ Similarly, claim 15 of the ’088 Patent recites “physical access control rules that are organized into two or more types of policies comprising system, user,

¹ In this declaration, all emphasis within quotations is added unless otherwise noted.

and **sensor state related policies**.” Replacing these terms with Vector Flow’s proposed construction renders these claims unclear and confusing.

6.3. Term 3: “native data representation format” (’704 Patent, cls. 11, 13)

HID’s Proposed Construction	Vector Flow’s Proposed Construction
No construction necessary; Plain and ordinary meaning	“the original format of the data transmitted by a sensor in response to a physical stimulus”

37. In my opinion, Term 3 should be construed in accordance with its plain and ordinary meaning.

38. The ’704 Patent, claim 11 recites, in pertinent part:

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;

In addition, dependent claim 13 is shown below:

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.

39. POSITAs understand that a “native data representation format” is a data format associated with a sensor. The claim language makes this clear: “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.” ’704 Patent at cl. 11.

40. The extrinsic evidence would have further guided a POSITA's understanding of the term "native," which is a common, readily understood term. For example, a technical dictionary linked the term to a particular device, which in the context of the '704 Patent, is the claimed sensor:

native data type (data management) A data type that is built into a software or hardware system. (C) 610.5-1990

Ex. 10 (The IEEE Standard Dictionary of Electrical and Electronics Terms) (1996).

41. In my opinion, Vector Flow's proposed construction is incorrect for multiple reasons. *First*, it requires that the native data be "data transmitted by a sensor in response to a physical stimulus," which is the same definition Vector Flow proposes for "sensor data." But Term 3 does not recite "sensor data," and therefore, Vector Flow's proposed construction wrongly imports an additional limitation that is not even tied to the claim language at issue. *Second*, given that Vector Flow's proposed construction for Term 3 includes its proposed construction of "sensor data," I disagree with Vector Flow's proposed construction for Term 3 for the same reasons as discussed in connection with Terms 1 and 2. *Third*, I disagree with Vector Flow's inclusion of "original format" in its proposed construction. It is unclear what Vector Flow means by "original format," but assuming Vector Flow means the format of the sensor data produced by the sensor, then this part of its construction is, at best, unnecessarily duplicative. The language of claim 11 already describes that the "native data representation format" is the data format "of each respective manufacturer of the plurality of manufacturers." '704 Patent at cl. 11.

6.4. Term 4: "integration module" ('704 Patent, cl. 11)

HID's Proposed Construction	Vector Flow's Proposed Construction
No construction necessary; Plain and ordinary meaning; Not indefinite	Indefinite

42. In my opinion, Term 4 is not indefinite and should be construed in accordance with its plain and ordinary meaning.

43. The '704 Patent, claim 11 recites, in pertinent part, “accepting sensor data from each security sensor **an integration module** including an agent for each type of security sensor.” Here, the plain language of claim 11 reflects that the “integration module” is a system component that: (1) accepts sensor data from each security sensor; and (2) includes an agent for each type of security sensor.

44. The '704 Patent specification describes the “integration module” similarly. *First*, I note that the '704 Patent specification states:

other, or to network **110** separately. Throughout the description, the terms, “module,” “component,” and “process” may be used interchangeably to mean an computer program, routine, or subroutine that is executed on any of the server and/or client computers of FIG. 1A, and may be implemented as software, firmware, or programmed hardware.

'704 Patent at 6:26-31. As such, pertinent portions of the specification may describe an “integration module,” “integration process,” “integration framework component,” or integration processes performed by an “integration layer.” *See, e.g., id.* at 7:41-45, 8:9-19; 12:26-50, 12:46-48.

45. *Second*, for another embodiment, the specification describes that:

facilities **102** and **104**. The integrated physical security management process includes functional components that perform the tasks of integrating non-standard and proprietary data from disparate and numerous sensor, alarm and moni-

toring systems within and among different facilities. In one embodiment, the integrated physical security management process **118** includes a normalization process that normalizes of disparate security systems data to a standard data format, for example, access control and alarm data. It also includes

'704 Patent at 4:65-5:5. *Third*, the specification further describes: “[p]hysical security systems 602 include various legacy physical access control systems (PACS) 604 that are **integrated through an integration process 605** that maps the legacy, proprietary data to standardized formats.” *Id.* at 12:26-36. *Fourth*, it describes that, in at least one embodiment, the “[d]ata formats [from field devices] are translated and mapped appropriately by **the integration module** for use by policies and applications.” *Id.* at 12:46-48.

46. In my opinion, a POSITA reading the claim in view of the specification would understand the scope of the “integration module” with reasonable certainty. As discussed above, the claim itself provides guidance on the scope of the term, and the specification further confirms that scope. In my opinion, the plain and ordinary meaning of “integration module” includes within its scope all of the embodiments described above.

6.5. Term 5: “individual user profiles” ('704 Patent, cl. 11)

HID's Proposed Construction	Vector Flow's Proposed Construction
No construction necessary; Plain and ordinary meaning	“a profile corresponding to an individual user”

47. In my opinion, Term 5 should be construed in accordance with its plain and ordinary meaning.

48. Claim 11 of the '704 Patent recites “defining **individual user profiles** and their respective access privileges and credentials in the system.” '704 Patent, cl. 11.

49. Term 5 consists of common, everyday words that would be readily understandable to a POSITA. I have reviewed the '704 Patent and it does not provide any special definition that would alter the term's ordinary, common usage. For example, the specification of the '704 Patent provides a few examples of what could constitute an "individual's profile" and each is consistent with the phrase's typical use:

assets (doors, buildings, etc). The disclosed system also provides processes and systems to generate unique physical access credentials for exclusive mapping between an individual's profile (job, department, location, etc) and an organizations spatial hierarchy of its global physical security system deployments (doors, buildings, etc), and generates unique access credentials based on individual profiles and automatic assignment across multiple physical security systems overcoming certain hardware/software limitations of standard access control system/hardware.

'704 Patent at 18:29-38.

50. The term "individual user profile" is also used consistently with the definition found in dictionaries:

user profile A set of preferences, settings, authorizations, email addresses, and the like, which is stored for each user of a multiuser system.

Ex. 9 (Wiley Electrical & Electronics Engineering Dictionary) (2004).

user profile *n.* A computer-based record maintained about an authorized user of a multiuser computer system. A user profile is needed for security and other reasons; it can contain such information as the person's access restrictions, mailbox location, type of terminal, and so on. *See also* user account.

Ex. 11 (Microsoft Computer Dictionary) (2002). In my opinion, the plain and ordinary meaning of "individual user profiles" includes within its scope all of these definitions.

51. In my opinion, there is no need to rearrange the order of the terms within this phrase, as Vector Flow proposes. Vector Flow seeks to narrow the scope of the phrase such that a single individual user corresponds to a specific profile. But the plain language of Term 5 does not limit the scope in such a manner.

6.6. Term 6: “common data representation format” (’704 Patent, cl. 11)

HID’s Proposed Construction	Vector Flow’s Proposed Construction
No construction necessary; Plain and ordinary meaning	“a data format that can be used by applications, rules engines and other standard software components, while still maintaining communication to the respective physical security systems, applications and devices in their native, proprietary format”

52. In my opinion, Term 6 should be construed in accordance with its plain and ordinary meaning.

53. Claim 11 of the ’704 Patent recites:

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;

54. In my opinion, the language of claim 11 itself already provides sufficient context on what the “common data representation format” is. In particular, claim 11 describes how the native data representation format of each manufacturer is mapped to a “common data representation format.” The claim language is unambiguous and need not be construed.

55. Vector Flow’s proposed construction appears to be based on a portion of the specification shown below:

It also normalizes the communication data, commands and events from the disparate physical security systems to a common standard format. This common representation can be used by applications, rules engines and other standard software components, while still maintaining communication to the respective physical security systems, applications and devices in their native, proprietary format. This eliminates the

'704 Patent at 7:46-52. However, this passage merely describes how “common data representation format” can be used by the systems in at least one embodiment. It does not provide a definition of “common data representation format” itself. For example, the clause starting with “while maintaining communication” describes system operations and does not even describe the concept of a “common data representation format.” It certainly is not a clear definition of the disputed claim term, nor does it clearly express an intent to redefine the term.

6.7. Term 7: “policy” / “policies” ('704 Patent, cls. 11,; '088 Patent, cls. 15-17, 19)

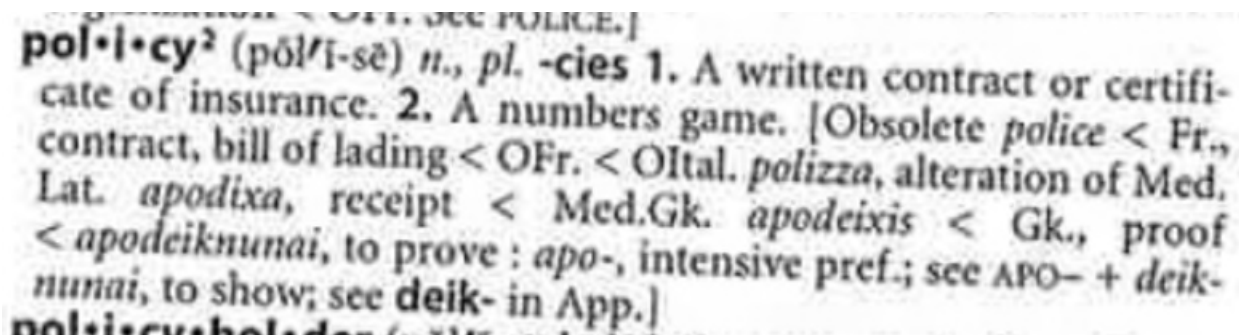
HID's Proposed Construction	Vector Flow's Proposed Construction
No construction necessary; Plain and ordinary meaning	“a user-defined logical entity that acts as a container for rules that are contained in the policy definition and allows easy grouping of rules in order to understand, view, enable and order them as one group”

56. In my opinion, Term 7 should be construed in accordance with its plain and ordinary meaning.

57. The Asserted Claims use the terms “policy” and “policies” in various contexts and formats. For example, claim 11 of the '704 Patent recites “physical security **policies**,” and claims 15-17 and 19 of the '088 patent recite “**policies** established for entity personnel,” “two or more types of **policies**,” “sensor state related **policies**,” “a graphical visual **policy** editor,” and “**policy** violations.” Similarly, the words “policy” and “policies” appear over a hundred times throughout the Asserted Patents’ specifications, and are most often used as part of generalized discussions of the system features.

58. In my opinion, the claim language, as written, already provides sufficient context on what the claims mean when it uses the terms “policy” and “policies.” For example, claim 11 of the ’704 Patent already recites that the “security policies” “define standardized rule definitions ... that are applied to the actionable events ... to produce normalized event data.” ’704 Patent, cl. 11. Similarly, claim 15 of the ’088 Patent already recites that its “defin[ed] policies” act to “control a data flow in accordance with the physical access control rule.” ’088 Patent, cl. 15.

59. Consistent with the generalized discussions of “policy” in the specifications, a POSITA understands that the term “policy” has a basic meaning that simply involves, for example, a plan of what actions to take in specified situations. The extrinsic evidence supports that understanding:



Ex. 12 (American Heritage College Dictionary) (2002). The Asserted Patents do not alter this common usage of the terms “policy” and “policies.”

60. Vector Flow’s proposed construction appears to come from two identical passages found within each of the Asserted Patents:

tem. A policy is a user-defined logical entity that acts as a container for rules that are contained in the policy definition. An administrator typically creates a policy and then adds rules to the policy. Multiple policies can be created in the system. Policies are logical entities that allow easy grouping of rules in order to understand, view, enable and order them as one group. Rules are the actual lowest level combination of Condition-Action that is applied to the data objects processed by the system. The policy manager applies one rule at a time to the data passing through the system.

'704 Patent at 11:41-51; '088 Patent at 13:7-16. Similar passages are also found later in each patent. *See* '704 Patent at 13:17-30; '088 Patent at 19:37-49.

61. The above passages are found at the end of the descriptions of the embodiments of Figures 4 and 6 in each patent. In my opinion, the above passages provide a generalized introduction to nature of the “policies.” They do not, as Vector Flow appears to believe, provide an express definition of the terms “policy” and “policies,” which, as discussed above, are recited throughout the Asserted Claims in different variations. For example, most of the language in the above passages describes how policies are used by the system in at least one embodiment, such as by acting “as a container for rule” or to “group[] rules.” But these passages do not define what each of the policies recited in the claims are. Rather, as discussed above, the claims themselves provide that context. In my opinion, the above passages are not clear definitions of the terms “policy” and “policies,” nor do they clearly express an intent to redefine the terms, as would be required for lexicography.

62. In addition, given the Asserted Claims use the terms “policy” and “policies” in various contexts and formats, then similar as discussed for Terms 1 and 2, Vector Flow’s proposed construction would also lead to confusion because it cannot be coherently inserted into the Asserted Claims.

6.8. Term 8: “rule” / “rules” (’704 Patent, cls. 11, 14, 15; ’088 Patent, cls. 15-17)

HID’s Proposed Construction	Vector Flow’s Proposed Construction
No construction necessary; Plain and ordinary meaning	“the actual lowest level combination of Condition-Action that is applied to the data objects processed by the system”

63. In my opinion, Term 8 should be construed in accordance with its plain and ordinary meaning.

64. The terms “rule” and “rules” appear through the Asserted Claims in various contexts and formats. For example, the ’704 Patent recites “wherein the security policies define standardized **rule** definitions through visual **rules**” (cl. 11), “applying relevant transformation and routing **rules** comprising condition action sequences” (cl. 11), “applying, through a **rules** engine, defined **rules** on the data and commands from each security sensor” (cl. 14), and “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” (cl. 15). Likewise, claim 15 of the ’088 Patent recites “constructing a **rule** from the first plurality of objects and second plurality of objects through connectors that dictate process flow by the first and second plurality of objects,” “executable **rules**,” and “physical access control **rules** of the managed site.” In my opinion, the claim language, as written, already provides sufficient context on what the claims mean when it uses the terms “rule” and “rules.”

65. The claims’ use of the terms “rule” and “rules” is consistent with a POSITA’s understanding of “rule,” which is a common English word that involves, for example, a definition of what is to be done in specified situations. The Asserted Patents do not alter this common usage of the terms “rule” and “rules.”

66. Vector Flow's proposed construction appears to come from one of the many different descriptions of "rules" used in connection with different embodiments throughout the Asserted Patents, namely:

one group. Rules are the actual lowest level combination of Condition-Action that is applied to the data objects processed by the system. The policy manager applies one rule at a time

'704 Patent at 11:48-50, '088 Patent at 13:13-15.

one group. Rules are the actual and lowest level combination of Condition-Action sequences that are applied to the data objects passing through the process. The policy manager

'704 Patent at 13:67-14:2, '088 Patent at 20:19-21.

67. However, Vector Flow's proposed construction appears to ignore other discussions of "rules" used in connection with other embodiments throughout the Asserted Patents, such as:

Rules are logically composed of separate components that facilitate the creation of complex expressions that are processed internally by the policy manager. A source to destina-

'704 Patent at 14:10-12, '088 Patent at 20:29-31.

Every rule has an action associated with it. A rule can have multiple actions defined for it that are performed when the condition specified in the rule matches it. All actions are performed exclusively and do not depend on the other actions defined for that rule. Action objects typically act as forward-

'704 Patent at 16:3-7, '088 Patent at 22:23-27.

68. I disagree with Vector Flow's proposed construction. For one, Vector Flow's proposed construction contradicts the claim language, at least because claim 11 of the '704 Patent already recites that the "rules compris[e] condition-action sequences." There is no requirement

that the rules be the “lowest level combination of Condition-Action,” and Vector Flow is improperly importing that requirement based on the specification.

69. In addition, in my opinion, the above passages do not provide an express definition of the terms “rule” and “rules,” which, as discussed above, are recited throughout the Asserted Claims in different variations. Rather, the above passages provide generalized introductions to the nature of the “rules” and how they are used by the system in at least one embodiment, but are not clear definitions of the terms “rule” and “rules,” nor do they clearly express an intent to redefine the terms. In my opinion, the claims themselves provide sufficient context on how they are using the terms “rule” and “rules.” In my opinion, the plain and ordinary meaning of Term 8 includes within its scope all of the embodiments described above.

70. In addition, given the Asserted Claims use the terms “rule” and “rules” in various contexts and formats, then similar as Terms 1, 2, and 7, Vector Flow’s proposed construction would also lead to confusion because it cannot be coherently inserted into the Asserted Claims.

6.9. Term 9: “visual rules” (’704 Patent, cl. 11)

HID’s Proposed Construction	Vector Flow’s Proposed Construction
No construction necessary; Plain and ordinary meaning	“a rule that is visually defined and depicted in a display area by placing icons and connectors in appropriate relationships to one another”

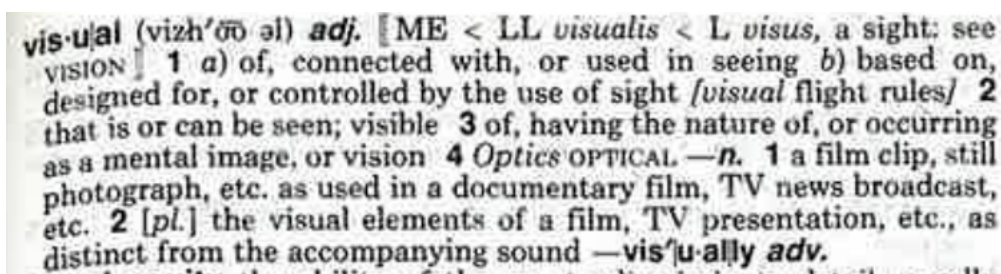
71. In my opinion, Term 9 should be construed in accordance with its plain and ordinary meaning.

72. Claim 11 of the ’704 Patent recites “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.” The claim language recites the scope of the term “visual rules,” and makes clear that they are “depicted by live objects that *contain attributes to define their spatial relationship to the actionable representations.*” This is

consistent with the specification, which recites that “**visual rule** objects *contain attributes that define their spatial relationship to other building blocks that are used to represent normalized systems, data and processes.*” ’704 Patent at 11:10-13.

73. POSITAs understand, from this intrinsic evidence, the scope of the term “visual rules.” In my opinion, the term should not be limited to this single excerpt from the specification, as Vector Flow proposes in its construction, because that excerpt is not a definition.

74. Additionally, as explained above at Term 8, POSITAs understand the plain and ordinary meaning of the term “rules.” Here, in Term 9, the additional word “visual” is also a basic term that POSITAs understand simply relates to vision and sight.



Ex. 13 (Merriam-Webster’s Collegiate Dictionary) (2004).

6.10. Term 10: “live objects” (’704 Patent, cl. 11)

HID’s Proposed Construction	Vector Flow’s Proposed Construction
Plain and ordinary meaning; “stencil objects”	“stencil shapes that are used to represent normalized systems, data and processes”

75. In my opinion, Term 10 should be construed in accordance with its plain and ordinary meaning. If desired, Term 10 could be construed as “stencil objects,” consistent with its plain and ordinary meaning.

76. Claim 11 of the ’704 Patent recites “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.” The specification states:

and other systems. The visual rule objects contain attributes that define their spatial relationship to other building blocks that are used to represent normalized systems, data and processes. Such building blocks are also referred to as stencil shapes or live objects.” The rule objects represent normalized

’704 Patent at 11:10-14.

77. The specification has several additional passages that refer to “stencil objects.” ’704 Patent at Abstract, 2:59-61, 3:26-31, 3:37-43, 16:49-51, 17:17-19, 17:22-24, 17:55-18:4; Figs. 8-11 (and associated descriptions). Based on the specification, a POSITA would understand that the patent uses the terms “stencil shapes” and “live objects” interchangeably. As such, it is my opinion that the term “live objects” could also be construed as “stencil objects,” consistent with the term’s plain and ordinary meaning.

78. Term 10 also uses the term “objects.” The term “object” is a common term that a POSITA would readily understand.

- object (1) (A)** Pertaining to the outcome of an assembly or compilation process. *See also:* object code; object module; object program. **(B)** A program constant or variable. **(C)** An encapsulation of data and services that manipulate that data. *See also:* object-oriented design. (C) 610.12-1990
- (2)** A data object that has an identifier (name) and a value. (C/LM) 802.10-1992
- (3)** A passive entity in a system that contains or receives information. Typically, objects include files, directories, registers, buffers, cache, memories, bus lines, displays, and other input/output devices. (BA/C) 896.3-1993
- (4)** A piece of data that can be defined by the operations performed on it. The Intrinsics represent an object internally as a pointer to a dynamically allocated data structure. (C) 1295-1993
- (5)** A representation of a real-world entity. An object is an instance of a class and has values for the attributes and relationships defined for that class. (C/SE) 1420.1-1995
- (6)** An abstraction of a physical or logical resource. (C) 610.7-1995
- (7)** An instance in the software hierarchy that can be operated on using the software administration utilities. (C/PA) 1387.2-1995
- (8)** Any of the complex information objects created, examined, modified, or destroyed by means of the[OM] interface. (C/PA) 1224-1993, 1224.1-1993, 1238.1-1994, 1327-1993, 1328-1993
- (9)** *See also:* directory object; OM object. (C/PA) 1224.2-1993, 1328.2-1993

Ex. 10 (The IEEE Standard Dictionary of Electrical and Electronics Terms) (1996).

79. Vector Flow's proposed construction appears to be based on the portion of the specification at 11:10-14 quoted above stating that visual rule objects are "used to represent normalized systems, data and processes." Again, in my opinion, this passage does not provide an express definition of the terms "live object" or "stencil object," but rather describes how they are used by the system in at least one embodiment. In my opinion, the claims themselves already provide sufficient context reciting how the "live objects" or "stencil objects" are used.

6.11. Term 11: “actionable representations” (’704 Patent, cl. 11)

HID’s Proposed Construction	Vector Flow’s Proposed Construction
No construction necessary; Plain and ordinary meaning	“a visual representation of actionable events that are defined in a visual policy engine for rules execution”

80. In my opinion, Term 11 should be construed in accordance with its plain and ordinary meaning.

81. Claim 11 of the ’704 Patent recites “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.”

82. Similarly, the specification of the ’704 Patent states:

As shown in FIG. 4, physical security policies are defined in a visual policy manager 420 using actionable representations of physical, network and IT systems as defined and configured in the system. Users, such as security administrators, define the data and event flow through the various physical security systems, rules that are run on it and the actionable events that are created from a policy engine as a result of rules execution. The rules thus defined are converted in step 412

’704 Patent at 10:24-31. This description references “actionable representations” in the embodiment of Figure 4 in a non-limiting manner, consistent with a POSITA’s understanding.

83. Term 11 includes two basic English terms that POSITAs readily understand when reading the claim language in light of the specification. A POSITA would understand that the term “actionable representations” means representations that are capable of being acted on. The extrinsic evidence supports that understanding:

Henahan
ac-tion-able \ˈak-sh(ə)-nə-bəl/ *adj* (1591) 1 : subject to or affording ground for an action or suit at law 2 : capable of being acted on <information> — **ac-tion-ably** \-blē/ *adv*
... (1972) ... a film dominated by a high degree

Ex. 13 (Merriam-Webster's Collegiate Dictionary) (2004).

84. Vector Flow's proposed construction replaces the straightforward, two-word term from the claims with a collection of 17 words selected from the portion of the specification shown above. In doing so, Vector Flow takes words from separate sentences and rearranges and combines them in order to craft a proposed construction that improperly imports multiple limitations into the claims. In my opinion, the above portion of the specification does not provide an express definition of, or evidence an intent to, clearly define the term "actionable representation." Rather, it describes that in at least one embodiment, the actionable representations are, among other things, "of physical, network and IT systems." '704 Patent at 10:24-27. This sentence does not define what the actionable representations are, as Vector Flow apparently contends. Moreover, it is unclear why Vector Flow uses only these two passages (which are from separate sentences) and ignores the rest of the passage. Accordingly, I disagree with Vector Flow's proposed construction.

6.12. Term 12: "spatial relationship" ('704 Patent, cls. 11, 15)

HID's Proposed Construction	Vector Flow's Proposed Construction
No construction necessary; Plain and ordinary meaning	"relationship in physical space"

85. In my opinion, Term 12 should be construed in accordance with its plain and ordinary meaning.

86. The claims of the '704 Patent use the term "spatial relationship" multiple times. Independent claim 11 recites:

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 representation format to produce normalized event data; and

Dependent claim 15 recites:

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.

In each of these claims, the term “spatial relationship” refers to a relationship between features that are *not physical*. Similarly, the specification uses the term once, and there too, refers to a *non-physical* spatial relationship between “objects” and “other building blocks that are used to represent normalized systems, data and processes.” ’704 Patent at 11:10-13.

87. This is in contrast to how another term “spatial hierarchy” is used in the ’704 Patent. The ’704 Patent uses that term in the physical context, as shown below:

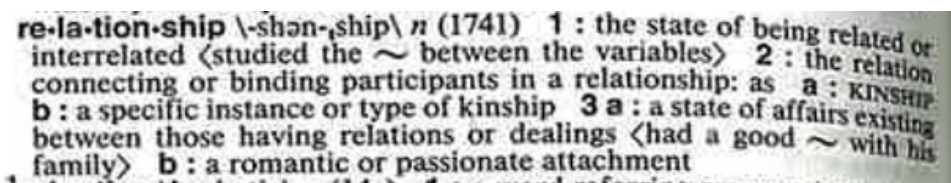
other physical security, network and IT systems. In this way, processes and systems are provided to discover and define an organizations spatial hierarchy of its global physical security assets (doors, buildings, etc). The disclosed system also provides processes and systems to generate unique physical access credentials for exclusive mapping between an individual's profile (job, department, location, etc) and an organizations spatial hierarchy of its global physical security system deployments (doors, buildings, etc), and generates unique access credentials based on individual profiles and automatic assignment across multiple physical security systems overcoming certain hardware/software limitations of standard access control system/hardware.

88. This intrinsic evidence makes clear that the term “spatial relationship” is not limited to a “relationship in physical space,” as Vector Flow proposes in its construction. POSITAs reading this record would understand that the full scope of the term captures both that which is physical and that which is not.

89. This conclusion is consistent with how the extrinsic evidence treated the term “spatial.” For example, a 2002 Microsoft Computer Dictionary defined the term “spatial data management” as follows:

spatial data management *n.* The representation of data as a collection of objects in space, particularly as icons on a screen, in order to make the data easier to comprehend and manipulate.

Ex. 11. Like the specification, this definition does not refer to physical space at all, but instead, refers to “a collection of objects” or “icons on a screen.” The only other word within Term 12 is “relationship.” But that too is a basic term, with a basic definition:



Ex. 13 (Merriam-Webster's Collegiate Dictionary) (2004).

6.13. Term 13: "routing rules" ('704 Patent, cl. 11)

HID's Proposed Construction	Vector Flow's Proposed Construction
No construction necessary; Plain and ordinary meaning	"a rule that controls the flow of data between different connected systems"

6.14. Term 14: "transformation rules" ('704 Patent, cl. 11)

HID's Proposed Construction	Vector Flow's Proposed Construction
No construction necessary; Plain and ordinary meaning	"a rule that defines and maintains the transformational mapping of data and events between different connected systems"

90. In my opinion, Terms 13 and 14 should be construed in accordance with their plain and ordinary meanings.

91. Terms 13 and 14 are recited in claim 11 of the '704 Patent together, as "transformation and routing rules." The scope of that phrase is set forth in the claim:

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.

Thus, POSITAs would have been informed of the plain and ordinary meaning of this term from the claim language itself, and further, by the consistent treatment of the term throughout the specification:

maintained for all physical security access and events. In one embodiment, this subcomponent includes a system orchestration framework 324 that defines and maintains the matrix of interconnectivity between disparate systems and proprietary data formats; a workflow, transformation and routing module 322 that defines and maintains the transformational mapping of data and events between the different connected systems, and also controls the flow of data between systems through rules based routing as defined by certain physical security policy process, states and actions 320. The rules-

...

IT applications are sent to the system for processing. The workflow module 424 then applied relevant transformation and routing rules to the events and data to generate action events 410 (for example, alerts, emails or SNMP alarms) on the physical security related actionable data (for example, personnel credentials and access privileges).

'704 Patent at 9:15-24, 10:51-56. In view of this intrinsic evidence, it is my opinion that there is no basis for requiring that there be separate rules for routing and separate rules for transformation, as Vector Flow proposes in its construction.

92. In my opinion, Vector Flow's proposed construction is also incorrect because it imports the above passages from 9:15-24 of the specification. However, that passage is directed to "one embodiment," so does not represent the full scope of these terms. Additionally, the passage is not a definition because it describes what a "rule" does (*i.e.*, it "controls" "defines and maintains"), but they do not define what a rule is.

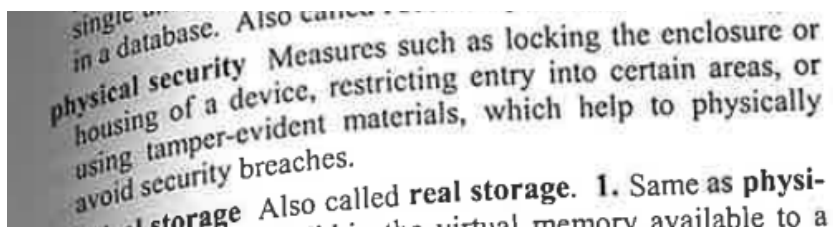
6.15. Term 15: "physical security" ('704 Patent, cl. 11; '088 Patent, cls. 15, 16)

HID's Proposed Construction	Vector Flow's Proposed Construction
No construction necessary; Plain and ordinary meaning	"security of a physical site"

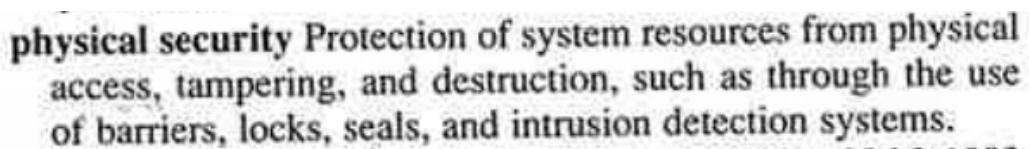
93. In my opinion, Term 15 should be construed in accordance with its plain and ordinary meaning.

94. The term “physical security” appears through the Asserted Claims in various contexts and formats. Claim 11 of the ’704 Patent recites, for example, “physical security policies” and “physical security states.” Claim 15 of the ’088 Patent recites, for example, “physical security data” and “physical security state engine.”

95. The specifications of the Asserted Patents provide several straightforward descriptions of “physical security systems,” noting for example, that they include “equipment and processes that implement physical security measures for incidents, access control, monitoring systems, lighting, security, audits, inspection, facility management, building automation, and the like.” ’704 Patent at 1:31-35; ’088 Patent at 1:30-34. These descriptions are consistent with a POSITA’s understanding of the term “physical security,” which is a common, readily understood term, as evidenced by its appearance in several technical dictionaries:



Ex. 9 (Wiley Electrical & Electronics Engineering Dictionary) (2004).



Ex. 10 (The IEEE Standard Dictionary of Electrical and Electronics Terms) (1996).

96. In my opinion, the plain and ordinary meaning of “physical security” includes within its scope all of the embodiments and definitions described above, and Vector Flow’s proposed construction is incorrect because it unnecessarily rearranges the words and adds a

limitation to narrow the meaning of this term. Vector Flow’s limitation that “security” must be directed to a physical “site” excludes security that may be generally related to a physical site, but does not rise to the level of specificity of “security of a physical site.”

6.16. Term 16: “physical security state” / “physical security states” (’704 Patent, cl. 11; ’088 Patent, cls. 15, 16)

HID’s Proposed Construction	Vector Flow’s Proposed Construction
No construction necessary; Plain and ordinary meaning	“information describing the status of physical security access and events”

6.17. Term 17: “security state” / “security states” (’704 Patent, cl. 11; ’088 Patent, cls. 15, 16)

HID’s Proposed Construction	Vector Flow’s Proposed Construction
No construction necessary; Plain and ordinary meaning	“information describing the status of security access and events”

97. In my opinion, Terms 16 and 17 should be construed in accordance with their plain and ordinary meanings.

98. Terms 16 and 17 appear through the Asserted Claims in various contexts and formats. For example, claim 11 of the ’704 Patent recites “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.” Claim 15 of the ’088 Patent recites “defining a first plurality of objects representing actors, facilities, *physical security states*, and network resources,” “build a continually updated *security state* of the entire system through alarm event messages generated by the network resources,” and “*physical security state* engine.” Again, Vector Flow’s proposed construction does not appear to take into account the different claims’ uses of Terms 16 and 17. In my opinion, the claim language, as written, already provides sufficient context on what the claims mean when it uses these terms.

99. The specifications provide additional guidance for this term. For example, the ’704 Patent recites:

propagated or generated by the system. The physical security policy process, states and actions module 320 receives the rules XML definitions from a visual policy manager and applies these definitions to the data and event flow occurring through the system. This module is also responsible for maintaining all physical security states (such as access permissions, alerts status and actual physical status of individuals in security systems). This state information is correlated to data changes and events processed through it and used to create actionable data changes and events affecting the state of relevant physical security, network and IT systems. A data

'704 Patent at 9:28-38. Vector Flow's proposed construction appears to be from another portion of the specification, which recites that the "rules determine the action to be taken and eventually the state that should be maintained for all physical security access and events." '704 Patent at 9:13-15; '088 Patent at 10:49-52. This disclosure, however, describes one function of "rules," and does not limit physical security states and security states to security "access and events."

100. Additionally, the following passage of the '088 Patent recites:

The network interfaces component includes a network command and query interface that allows querying of security state information by network and IT equipment in real-time to affect network data transmission and IT applications access in real-time. The physical security services can directly affect

'088 Patent at 9:14-18. But this reference to "security state information" does not mean that the "security state" is limited to information, as Vector Flow proposes in its construction.

101. The intrinsic evidence is consistent with a POSITA's understanding of Terms 16 and 17. These terms are phrases that include basic terms that are well-understood to a POSITA. For example, as discussed above at Term 15, the term "physical security" appears in several

technical dictionaries that POSITAs would have referenced. Likewise, as shown below, one of those technical dictionaries further provides basic definitions for the terms “security” and “state.”

security 1. The measures and techniques utilized to safeguard against losses, damage, unwanted modifications, or unauthorized access. Used, for instance, in the context of computers and communications. Examples include computer security, data protection, and network security. 2. The act of providing **security** (1). Also the condition of having such security.

state 1. A description of the conditions or circumstances of a particle, entity, or system, which encompasses one or more key attributes. Also, such a state. For example, a ground state, an excited state, or a quantum state. 2. The condition in which a component, circuit, device, piece of equipment, system, material, process, or setting is in at a given moment. For example, and idle state, or a logic state. 3. The condition in which a computer program, device, system, setting, sequence, or the like is in at a given moment. 4. Same as state of matter.

Ex. 9 (Wiley Electrical & Electronics Engineering Dictionary) (2004).

102. In my opinion, the plain and ordinary meaning of Terms 16 and 17 includes within its scope all of the embodiments and definitions described above.

6.18. Term 18: “single integration layer component” (’088 Patent, cl. 15)

HID’s Proposed Construction	Vector Flow’s Proposed Construction
No construction necessary; Plain and ordinary meaning; Not indefinite	Indefinite

103. In my opinion, Term 18 is not indefinite and should be construed in accordance with its plain and ordinary meaning.

104. Claim 15 of the ’088 Patent recites:

receiving, in a single integration layer component from each of the plurality of objects in the proprietary data format of a respective security component and integrate disparate proprietary data formats for aggregation and processing in other components;

105. As shown above, the claim language itself reflects that the “single integration layer component” is a system component that receives and integrates disparate propriety data formats from respective security components for use by other components.

106. Again, the '088 Patent's specification describes the single integration layer similarly. For example, the specification describes:

networking systems. An integration layer contains agents and adapters with built-in intelligence for multiple physical security systems and supports extensibility through mapping of application protocols, command and data **152** formats for integration with new and emerging physical security systems. It also normalizes the communication data, commands and events from the disparate physical security systems to a common standard format. This common representation can be

'088 Patent at 7:59-66.

107. In my opinion, a POSITA reading the claim in view of the specification readily understand the scope of the “single integration layer component” with reasonable certainty. As discussed above, the claim itself provides guidance on the scope of the term, and the specification further confirms that scope. In my opinion, the plain and ordinary meaning of “single integration layer component” includes within its scope all of the embodiments described above.

6.19. Term 19: “protocol defined trap message” ('088 Patent, cl. 15)

HID's Proposed Construction	Vector Flow's Proposed Construction
No construction necessary; Plain and ordinary meaning	“an unsolicited alert message defined by Simple Network Management Protocol”

108. In my opinion, Term 19 should be construed in accordance with its plain and ordinary meaning.

109. Claim 15 of the '088 Patent recites:

extracting physical security data and events from network traffic and the security components to build a continually updated security state of the entire system through alarm event messages generated by the network resources, wherein the alarm event messages are generated by a protocol defined trap message and a system log daemon process aggregates the alarm event messages;

110. The specification states:

SNMP Alarm Event (Trap):

The following example defines an alarm (Trap in SNMP terminology) which is generated by a network device (system or application) containing details in the objects defined in it. The receiving party uses information such as this to understand the format of the data received in the trap and thus create actions and rules to respond to it.

'088 Patent at 15:62-67.

111. This description refers to an “example” that “defines an alarm” which is referred to as a “Trap in SNMP terminology.” This description does not limit a “protocol defined trap message” to only (1) “an unsolicited” (2) “alert message” that is (3) “defined by Simple Network Management Protocol,” as Vector Flow proposes in its construction. Rather, this portion of the specification describes an “example” and confirms that a trap message can refer to a message using the Simple Network Management Protocol. This is consistent with a POSITA’s understanding of “protocol defined trap message.” POSITAs understand that this term includes a protocol defined message associated with an exception that occurs in software. That understanding is further consistent with a technical dictionary definition of the term “trap,” as shown below:

(3) (A) (software) A conditional jump to an exception or interrupt handling routine, often automatically activated by hardware, with the location from which the jump occurred recorded. (B) (software) To perform the operation in definition (A). (C) 610.12-1990

Ex. 10 (The IEEE Standard Dictionary of Electrical and Electronics Terms) (1996).

6.20. Term 20: “system log daemon” (’088 Patent, cl. 15)

HID’s Proposed Construction	Vector Flow’s Proposed Construction
No construction necessary; Plain and ordinary meaning	“a server process that provides a message logging facility for systems”

112. In my opinion, Term 20 should be construed in accordance with its plain and ordinary meaning.

113. Claim 15 of the ’088 Patent recites:

extracting physical security data and events from network traffic and the security components to build a continually updated security state of the entire system through alarm event messages generated by the network resources, wherein the alarm event messages are generated by a protocol defined trap message and a system log daemon process aggregates the alarm event messages;

114. The specification of the ’088 Patent states:

Syslog Format:

Syslog is a method to collect messages from devices to a server running a syslog daemon. Logging to a central syslog server helps in aggregation of logs and alerts. Network vendor’s devices can send their log messages to a SYSLOG service.

’088 Patent at 16:15-20.

115. Based on this intrinsic evidence, POSITAs understand that a “system log daemon” refers to message logging for applications or system processes. This is consistent with several relevant technical dictionaries, one of which defined the term “daemon” as follows:

daemon Acronym for **disk and execution monitor**. A program which runs in the background and automatically performs administrative functions when needed, or at specified times. Examples of daemons include email handlers and print spoolers. Also spelled **demon**.

Ex. 9 (Wiley Electrical & Electronics Engineering Dictionary) (2004).

116. In my opinion, the plain and ordinary meaning of “system log daemon” includes within its scope all of the embodiments and definitions described above, and is not limited to only a “server process” and only message logging for a “system,” as Vector Flow proposes in its construction. Vector Flow’s proposed construction excludes processes on, *e.g.*, a computer, and excludes messages about, *e.g.*, an application.

6.21. Term 21: “build a continually updated security state” (’088 Patent, cl. 15)

HID’s Proposed Construction	Vector Flow’s Proposed Construction
No construction necessary; Plain and ordinary meaning	“proactively building the security state of a deployed and interconnected system by maintaining and continually updating the state of the system through normalized sensor data and executable rules”

117. In my opinion, Term 21 should be construed in accordance with its plain and ordinary meaning.

118. Claim 15 of the ’088 Patent recites:

extracting physical security data and events from network traffic and the security components to build a continually updated security state of the entire system through alarm event messages generated by the network resources,

119. As discussed above at Term 17, the term “security state” is a common term that is readily understood by a POSITA. The remaining words in Term 21 here are common English words that POSITAs also understand:

build \ˈbɪld\ *vb* **built** \ˈbɪlt\; **build-ing** [ME *bilden*, fr. OE *byldan*; akin to OE *būan* to dwell — more at **BOWER**] *vt* (bef. 12c) **1** : to form by ordering and uniting materials by gradual means into a composite whole : **CONSTRUCT** **2** : to cause to be constructed **3** : to develop according to a systematic plan, by a definite process, or on a particular base **4** : **INCREASE, ENLARGE** ~ *vi* **1** : to engage in building **2 a** : to progress toward a peak (as of intensity) <~ to a climax> **b** : to develop in extent <a crowd ~ing> — **build a fire under** : to stimulate to vigorous action — **build into** : to make an integral part of <build quality into the product> — **build on** : to use as a foundation <building on past experience>

Ex. 13 (Merriam-Webster’s Collegiate Dictionary) (2004)

con•tin•u•al (kən-tɪnˈyoʊ-əl) *adj.* **1.** Recurring regularly or frequently. **2.** Not interrupted; steady. — **con•tin•u•al•ly** *adv.*

up•date (ʊp-dātˈ) *tr.v.* -dat•ed, -dat•ing, -dates To bring up to date: *update the files.* ♦ *n.* (ʊpˈdātˈ) **1.** Information that updates something. **2.** The act or an instance of bringing up to date. **3.** An updated version of something.

Ex. 12 (The American Heritage College Dictionary) (2002).

120. In my opinion, the plain and ordinary meaning of Term 21 includes within its scope all of the embodiments and definitions described above, and should not be limited in the manner that Vector Flow proposes in its construction. Vector Flow imports the following excerpt from the prosecution history of the ’088 Patent:

In general, Prokupets only teaches chronologically storing data in an event log in a database, whereas the claimed invention recites proactively building the security state of a deployed and interconnected system by maintaining and continually updating the state of the system through normalized sensor data and executable rules. Thus, Prokupets does not teach a system that has components that “build a continually updated security state of the system through a physical security state engine,” but instead teaches the use of an access privileges lookup table in a central database. (Prokupets, Para. 0038).

Ex. 8.

121. I disagree with Vector Flow’s proposal for the following reasons. *First*, this is not a definition for this term, because it merely describes prior art. Nor does the statement disclaim subject matter. Instead, if anything, it enlarges the scope of the claim by describing an open-ended system and including another manner in which the claimed “build” occurs (*i.e.*, “through normalized sensor data and executable rules.”). This is broader than claim 15 of the ’088 Patent, which recites “build a continually updated security state of the entire system ***through alarm event messages generated by the network resources***.” *Second*, Vector Flow’s incorporation of these limitations changes the features that are already recited in the claim. *Third*, this statement was made with respect to claim 1, not claim 15. Specifically, this passage and claim 1 are directed to the “build” function “through a physical security state engine.” This limitation is not recited in claim 15.

6.22. Term 22: “physical security state engine” (’088 Patent, cl. 15)

HID’s Proposed Construction	Vector Flow’s Proposed Construction
No construction necessary; Plain and ordinary meaning	“A real-time, high speed repository and access interface to all the security states defined in the system”

122. In my opinion, Term 22 should be construed in accordance with its plain and ordinary meaning.

123. Claim 15 of the ’088 Patent recites:

building, in a physical security state engine, active access lists and states for physical access control systems through the extracted physical security data and the daemon process, wherein the active access lists define at runtime access information for individuals or groups of individuals defined within the system;

The specification's disclosure related to Term 22 states:

events. Rules-based event and data correlation results in actionable state information for IT, network and other security systems. The physical security state engine 326 within the PSS module 302 is the real-time, high speed repository and access interface to all the security states defined in the system.

'088 Patent at 10:52-56. This description does not disturb a POSITA's understanding of the plain and ordinary meaning of this term, which encompasses several terms that are readily understood by a POSITA, as discussed above at Terms 15-17. Rather, this description merely describes the functionality of "physical security state engine 326" as it is used within a specific embodiment. That description is consistent with extrinsic evidence, such as the following dictionary definition:

engine *n.* A processor or portion of a program that determines how the program manages and manipulates data. The term *engine* is most often used in relation to a specific use; for example, a database engine contains the tools for manipulating a database, and a Web search engine has the ability to search World Wide Web indexes for matches to one or more key words entered by the user. *Compare* back-end processor, front-end processor.

Ex. 11 (Microsoft Computer Dictionary) (2002).

124. Accordingly, in my opinion, the plain and ordinary meaning of Term 22 includes within its scope all of the embodiments and definitions described above, and should not be limited to the specific embodiment that Vector Flow proposes importing from the specification at

10:52-56.

6.23. Term 23: “virtual objects” (’088 Patent, cls. 15, 16)

HID’s Proposed Construction	Vector Flow’s Proposed Construction
No construction necessary; Plain and ordinary meaning; Not indefinite	Indefinite; “a visual depiction of an object that is not real”

125. In my opinion, Term 23 is not indefinite and should be construed in accordance with its plain and ordinary meaning.

126. Claim 15 of the ’088 Patent, recites in pertinent part:

normalizing the plurality of signals from each proprietary format to an Extensible Markup Language (XML) format to produce normalized signal data, wherein the XML format is configured to describe system policies through the use of virtual objects that comprise components of executable rules, and represents relationships between the virtual objects and corresponding devices, objects and processes, and wherein the schema defines

127. As shown above, the plain language of claim 15 reflects that “virtual objects” are used to describe system policies, “comprise components of executable rules,” and have relationships to the “corresponding devices, objects and processes.”

128. In my opinion, the term “virtual objects” consists of common English words that have meanings that are readily understood by a POSITA especially when read in view of the specification, and there is no reason to construe the terms as Vector Flow proposes. The specification describes a number of object types, such as “HTML objects,” “data objects,” “embeddable software objects,” and “stencil objects.” *See, e.g.*, ’088 Patent at 6:51-54, 8:29-33, 19:53-46, 20:5-7, 20:37-38, 23:37-44. Each of these types of objects are “virtual” in the sense that they are implemented by a computer system, but not all are “visual depictions,” nor are they all

“visual depictions of an object that is not real.” Indeed, some of the objects described in the ’088 Patent specification are graphical representations of objects that are real. For example, the ’088 Patent specification describes objects that are graphical representations and consist of “a graphic of a building for a site” or “a graphic of a person for an actor or personnel within the system” See, e.g., ’088 Patent at 21:11-16. Thus, the virtual object depicts an object that is real. Vector Flow’s construction wrongly excludes these embodiments.

129. In addition, I note that dependent claim 16 recites:

16. The method of claim 15 wherein the rule is constructed using a graphical visual policy editor that processes virtual objects, and wherein the physical security states and their relationships with network resources are managed and depicted as the virtual objects.

Id., cl. 16.

130. As shown above, claim 16 is directed to the concept of “a graphical visual policy editor that processes virtual objects” and “depict[s]” the virtual objects visually. Vector Flow’s proposed construction improperly incorporates these same concepts into claim 15 where they are not present.

6.24. Term 24: “reference” / “references” (’088 Patent, cl. 15)

HID’s Proposed Construction	Vector Flow’s Proposed Construction
No construction necessary; Plain and ordinary meaning; Not indefinite	“a shape used to create references for lookups for information”

131. In my opinion, Term 24 is not indefinite and should be construed in accordance with its plain and ordinary meaning.

132. Claim 15 of the ’088 Patent recites “defining a second plurality of objects representing actions, conditions and **references**.” The specification of the ’088 Patent uses this

term consistent with the English language, and consistent with a POSITA's understanding. For example, the specification states:

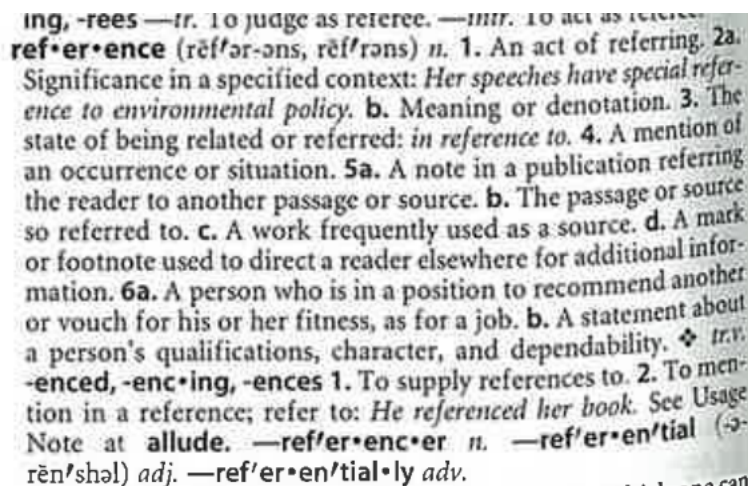
instance or other interconnection restriction. All shape behaviors and properties are defined when the shape is created. A number of basic types of shapes are utilized by the system: object shapes, condition shapes, actions shapes, modification shapes, references, and connectors.

...

ing or removing role-based access privileges. Reference shapes are used to create references for lookups and comparisons by the rules engine in real-time while processing the incoming data based on the preceding conditions. These

'088 Patent at 21:7-10, 21:34-37.

133. This usage is further consistent with extrinsic evidence that defines the term "reference" with basic definitions:



The image shows a close-up of a dictionary page. The word 'reference' is highlighted in bold. The definition includes: '1. An act of referring. 2a. Significance in a specified context: Her speeches have special reference to environmental policy. b. Meaning or denotation. 3. The state of being related or referred: in reference to. 4. A mention of an occurrence or situation. 5a. A note in a publication referring the reader to another passage or source. b. The passage or source so referred to. c. A work frequently used as a source. d. A mark or footnote used to direct a reader elsewhere for additional information. 6a. A person who is in a position to recommend another or vouch for his or her fitness, as for a job. b. A statement about a person's qualifications, character, and dependability. ♦ tr.v. -enced, -enc-ing, -ences 1. To supply references to. 2. To mention in a reference; refer to: He referenced her book. See Usage Note at allude. —refer-enc-er n. —refer-en'tial (-rən'shəl) adj. —refer-en'tial-ly adv.'

Ex. 12 (The American Heritage College Dictionary) (2004).

134. In my opinion, the plain and ordinary meaning of Term 24 includes within its scope all of the embodiments and definitions described above.

135. Vector Flow's proposed construction appears to be from the following portion of

the specification:

ing or removing role-based access privileges. Reference shapes are used to create references for lookups and comparisons by the rules engine in real-time while processing the incoming data based on the preceding conditions. These

'088 Patent at 21:34-37. But this sentence describes how to use a “reference shape,” it does not define a “reference.” Nor does Vector Flow’s proposed construction define the word “reference.”

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

Dated: October 27, 2022

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Mark Jones", written in a cursive style.

Mark Jones PhD