Trials@uspto.gov
Tel: 571-272-7822

Paper 27
Date: February 2, 2024

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

INTERNATIONAL BUSINESS MACHINES CORPORATION,
Petitioner,

v.

EBATES PERFORMANCE MARKETING, INC.
dba RAKUTEN REWARDS,
Patent Owner.

IPR2022-01250
Patent 7,962,960 B2

Before KEVIN F. TURNER, SCOTT A. DANIELS, and
KEVIN C. TROCK, *Administrative Patent Judges.*

TROCK, *Administrative Patent Judge.*

JUDGMENT
Final Written Decision
Determining Some Challenged Claims Unpatentable
35 U.S.C. § 318(a)

I. INTRODUCTION

We have authority to hear this *inter partes* review under 35 U.S.C. § 6. This Final Written Decision issues pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73. For the reasons discussed herein, we determine that Petitioner, International Business Machines Corporation ("Petitioner" or "IBM") has shown by a preponderance of the evidence that claims 1–5 and 7–22 of U.S. Patent No. 7,962,960 B2 (Ex. 1001, "the '960 patent") are unpatentable, but has not shown by a preponderance of the evidence that claim 23 is unpatentable. *See* 35 U.S.C. § 316(e) (2018); 37 C.F.R. § 42.1(d) (2019).

A. Background

IBM filed a Petition (Paper 2, "Pet.") to institute an *inter partes* review of claims 1–5 and 7–23 ("the challenged claims"). Ebates Performance Marketing, Inc. dba Rakuten Rewards ("Patent Owner") filed a Preliminary Response (Paper 6, "Prelim. Resp."). Based upon the record at that time, we instituted *inter partes* review on all challenged claims on the grounds presented in the Petition. Paper 7 ("Institution Decision" or "Dec.").

After institution, Patent Owner filed a Response (Paper 13, "PO Resp."), Petitioner filed a Reply (Paper 15, "Pet. Reply"), and Patent Owner filed a Sur-reply (Paper 20, "PO Sur-reply").

On November 6, 2023, an oral hearing was held and a transcript of the hearing was entered into the record. Paper 26 ("Transcript" or "Tr.").

B. Related Matters

The parties identify the following district court proceeding involving the '960 patent: *International Business Machines Corporation v. Rakuten, Inc., Rakuten USA Inc., Rakuten Commerce, LLC, and Ebates Inc. dba Rakuten*, 1:21-cv-00461 (D. Del.). Pet. 1; Paper 4, 2.

C. The '960 Patent

The '960 patent is titled "Systems and Methods for Performing Risk Analysis." Ex. 1001, code (54). The '960 patent relates to analyzing networks and network devices for vulnerabilities. *Id.* at 1:13–15. Figure 1 of the '960 patent is reproduced below.

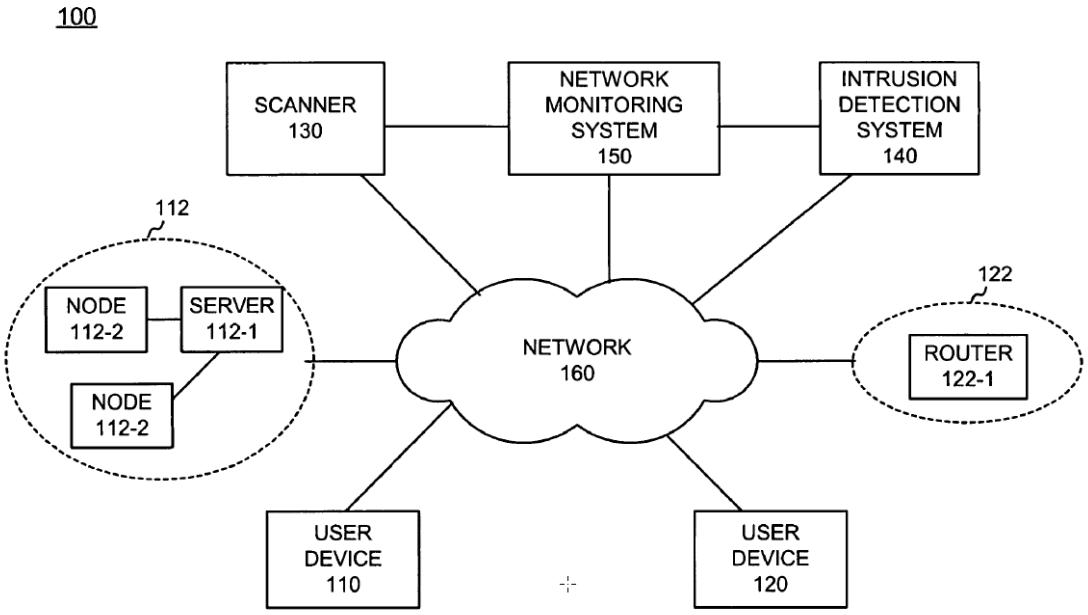


FIG. 1

Figure 1 is a block diagram depicting system 100 including user devices 110, 120; domains 112, 122; scanner 130; intrusion detection system (IDS) 140; network monitoring system 150; and network 160. *Id.* at 2:34–39.

The '960 patent explains that performing a risk analysis procedure via network monitoring system 150 may begin with associated personnel generating a list of potential vulnerabilities associated with network elements in system 100 and assigning each potential vulnerability a numerical value based on, e.g., the likelihood that the vulnerability can be exploited. *Id.* at 7:59–8:13. Scanner 130 may also detect anomalies in network devices, for example, by scanning a server for open ports that may be infiltrated by a hacker. *Id.* at 3:18–21; 9:19–24. Network monitoring system 150 performs a risk analysis associated with devices in system 100, by assigning numerical values associated with particular vulnerabilities in the system. *Id.* at 7:59–63. Network monitoring system 150 may receive the data from scanner 130, IDS 140 and/or other sources and correlate the information to generate an appropriate score or grade. *Id.* at 9:41–43. After a value has been assigned to each potential vulnerability associated with network elements in system 100, network monitoring system 150 may store this information in, for example, policy monitoring tools database 340. *Id.* at 8:61–64.

In one implementation, policy monitoring tools database 340 may store minimum security baseline (MSB) rules associated with devices in system 100. *Id.* at 5: 47–51. MSB rules may identify various minimum security policies or rules associated with devices in system 100. *Id.* Policy monitoring tools database 340 may also store "exception" information identifying both business and technical exceptions associated with various network devices. *Id.* at 5:48–50.

Network monitoring system 150 may correlate the information received from scanner 130 and IDS 140 with the "exception" information

when generating a score/grade for a network element. *Id.* at 9:51–54. The '960 patent explains, for example, that

> if a scan shows that a program is being run on server 112-1, such as a program that is not generally approved for server 112-1, network monitoring system 150 may determine whether an exception has been granted for that program to be run on server 112-1. If an exception has been granted, network monitoring system 150 may reduce the score associated with this network element. In addition, network monitoring system 150 may check the exception information in policy monitoring tools database 340 to determine whether any other exceptions associated with, for example, other anomalies in the type/amount of data that server 112-1 is receiving to determine whether the anomaly is covered by an exception that has been approved for that network element. The exception, therefore, may account for the anomaly. In an exemplary implementation, if an exception has been approved for a particular network element, the score for that particular network element may be reduced by some value, such as 50.

Id. at 9:56–10:6.

Exception information utilized by network monitoring system 150 may also involve technical exceptions. *Id.* at 10:7–8. The '960 patent explains

> [f]or example, assume that scanner 130 runs a scan on one of nodes 112-2 and the resulting scan data is meaningless or erroneous. Network monitoring system 150 may check policy monitoring tools database 340 to determine whether a business exception has been approved for node 112-2, such as information indicating that node 112-2 is using an operating system that is not compatible with scanner 130. If such an exception has been granted, network monitoring system 150 may reduce the score for node 112-2 by a predetermined amount, such as, for example, 50.

Id. at 10:9–18.

The '960 patent also explains that

> [a]fter network monitoring system 150 has received the information from scanner 130 and IDS 140 and has correlated the received data with information stored in, for example, policy monitoring tools database 340, asset database 320 and/or ownership database 330, network monitoring system 150 may generate a score for each network element (i.e., server 112-1 and nodes 112-2 in this example). For example, the values associated with each of the identified vulnerabilities for server 112-1 may be added to generate an overall score.

Id. at 10:25–34.

The '960 patent further explains that

> [a]fter scores, grades or some other relative risk indicator, (referred to collectively hereafter as risk level indicators) are generated for each identified network element in system 100, network monitoring system 150 may provide the risk level indicators to user device 110 (act 540). The risk level indicator may be an overall risk level indicator for domain 112 and/or a risk level indicator for each individual element in domain 112.

Id. at 10:61–11:1.

The '960 patent also describes how remediation actions may be performed in order to reduce a risk. For example, the network monitoring system may send an alert to a console associated with another party (e.g., a network engineer) associated with maintaining security for a particular server indicating that a security problem exists. If the risk is high enough, the network monitoring system may take actions to automatically quarantine the server to limit or halt traffic to/from the server. *Id.* at 11:34–44.

D. Challenged Claims

Petitioner challenges claims 1–5 and 7–23 of the '960 patent. Pet. 1. Claims 1, 12, 18, and 23 are independent and similar, with claims 1 and 12 directed to methods and claims 18 and 23 directed to systems. Claim 1 is

illustrative and is reproduced below, with Petitioner's bracketed designations added to the limitations for reference purposes.

> 1. [1Pre] A method comprising:
>
> [1A] at a network monitoring system of a computer network that comprises a plurality of network elements, wherein the network monitoring system includes a hardware processing device,
>
> [1B] receiving a plurality of values that each corresponds to a vulnerability of a network element of the plurality of network elements;
>
> [1C] storing, at the network monitoring system, information representing exceptions to security rules;
>
> [1D] scanning, by a scanning device, the plurality of network elements to identify vulnerabilities, the vulnerabilities representing potential points of attack;
>
> [1E] generating, by said network monitoring system, a risk indicator for each of the network elements based on the scanning and the received plurality of values, the risk indicator representing a relative risk level associated with the corresponding network element;
>
> [1F] determining, by the network monitoring system and subsequent to the generating a risk indicator, whether an exception to a security rule exists with respect to any of the identified vulnerabilities;
>
> [1G] adjusting, by the network monitoring system, the risk indicator for a first one of the network elements in response to determining that an exception to a security rule exists with respect to an identified vulnerability associated with the first network element; and
>
> [1H] providing the risk indicator for each of the network elements to a user device for display.

Ex. 1001, 15:10–37.

E. Evidence

The parties rely on the following evidence of record.

Reference or Declaration	Date	Exhibit No.
Declaration of Henry Houh, Ph.D.	July 13, 2022	Ex. 1002
Andres et al., U.S. Patent No. 8,201,257 B1 ("Andres")	June 12, 2012	Ex. 1003
Dodd et al., U.S. Patent Publication No. 2002/0147803 A1 ("Dodd")	Oct. 10, 2002	Ex. 1004
Njemanze et al., U.S. Patent No. 7,788,722 B1 ("Njemanze")	Aug. 31, 2010	Ex. 1005
Reply Declaration of Henry Houh, Ph.D.	Aug. 6, 2023	Ex. 1020
Declaration of Mark Crovella, Ph.D.	May 16, 2023	Ex. 2005

F. Asserted Grounds of Unpatentability

Petitioner challenges the patentability of claims of the '960 patent on the following grounds:[1]

Claims Challenged	35 U.S.C. §[2]	References
1–4, 7–12, 14–20, 22, 23	103(a)	Andres, Dodd
2, 5, 13, 21	103(a)	Andres, Dodd, Njemanze

Pet. 21.

III. ANALYSIS

A. Applicable Legal Standards

A claim is unpatentable as obvious under 35 U.S.C. § 103(a) (2010) "if the differences between the subject matter sought to be patented and the

[1] The Petition lists four grounds of unpatentability. Grounds III and IV are the same as Grounds I and II, except they are asserted "[u]nder Rakuten's claim interpretations, as laid out in Rakuten's Initial Infringement Contentions ("EX1007") in the related litigation." Pet. 85.

[2] The Leahy-Smith America Invents Act ("AIA"), Pub. L. No. 112-29, 125 Stat. 284, 287–88 (2011), amended 35 U.S.C. § 103, effective March 16, 2013. Because the '960 patent claims priority to a provisional application that was filed before this date, with Petitioner not contesting that priority, the pre-AIA version of § 103 applies. *See* Ex. 1001, code (60); Pet. 7.

prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains." The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) so-called "secondary considerations," including commercial success, long-felt but unsolved needs, failure of others, and unexpected results. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). Neither party has presented any evidence on the fourth *Graham* factor.

B. Level of Ordinary Skill in the Art

According to Petitioner, a person of ordinary skill in the art "would have been someone knowledgeable in information technology and networking" and "would have a bachelor's degree in electrical engineering, computer science, or equivalent training, and approximately 2 years of experience working in information technology and networking." Pet. 17–18 (citing Ex. 1002 ¶ 111). Without agreeing that it is proper, Patent Owner and its expert apply Petitioner's proposal. *See* PO Resp. 8 (citing Ex. 2002 ¶¶ 33–34.).

For the purposes of this Decision, we continue to use the same assessment offered by Petitioner that we adopted in our preliminary assessment of a person of ordinary skill in the art in the Institution Decision, as it is consistent with the '960 patent and the prior art before us. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001) (the prior art itself may reflect an appropriate level of skill).

C. Claim Construction

We construe each claim "in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent." 37 C.F.R. § 42.100(b). 37 C.F.R § 42.100(b) (2019). Under this standard, claim terms "are generally given their ordinary and customary meaning" as understood by a person of ordinary skill in the art in question at the time of the invention. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005) (en banc) (citations omitted). "In determining the meaning of the disputed claim limitation, we look principally to the intrinsic evidence of record, examining the claim language itself, the written description, and the prosecution history, if in evidence." *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 469 F.3d 1005, 1014 (Fed. Cir. 2006) (citing *Phillips*, 415 F.3d at 1312–17). Extrinsic evidence is "less significant than the intrinsic record in determining 'the legally operative meaning of claim language.'" *Phillips*, 415 F.3d at 1317 (citation omitted).

Only those terms that are in controversy need be construed, and only to the extent necessary to resolve the controversy. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017); *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999).

The Petition "applies the plain and ordinary meaning of claim terms," other than the "means-plus-function" limitations recited by independent claim 23. *See* Pet. 18–20. In its Response, Patent Owner indicates that "[t]he parties generally agree that all claim terms except the means-plus-

function limitations should be construed according to the plain and ordinary meaning . . . of those terms." PO Resp. 8–9.

1. Exception Limitations

Each of the challenged independent claims recite the phrase "exception to a security rule" and/or "exceptions to security rules." *See e.g.,* Ex. 1001, 15:18, 15:29. In its Response, Patent Owner asserts that the plain meaning of the phrase "exception to a security rule" is "an instance in which a security rule does not apply." *Id.* at 9.

Patent Owner asserts that "[t]he '960 patent does not set out any special definition of 'exception,' 'exception to a security rule,' or 'exceptions to security rules.'" *Id.* (citing Ex. 2005 ¶¶ 41–43). Patent Owner also indicates that "the '960 patent describes that exceptions to security rules may represent an 'anomaly' from general circumstances, or a situation in which a security rule may be permissibly violated such as once an administrator or manager grants approval for a violation." PO Resp. 9 (citing Ex. 1001, 5:58–6:15, 7:22–39, 9:51–10:18). Patent Owner asserts that "[a]n exception to a security rule can be associated with adjusting risk indicated by the security rule," and that "exceptions may indicate instances in which risk should be scored differently than what is specified by the general security rule and to which the security rule does not apply." PO Resp. 10.

In its Reply, Petitioner agrees with Patent Owner that the plain and ordinary meaning of the term "exception to a security rule" is "an instance in which a security rule does not apply," and that this agreed upon meaning is consistent with the '960 patent in that that "minimum security baseline *rules* may include minimum security *policies*." Pet. Reply 2–3.

Given the absence of a special definition of these phrases in the '960 patent, the '960 patent's indication that minimum security baseline rules may include minimum security policies, the lack of any testimony by the parties' experts contesting a general understanding of the term in the art, and the agreement by the parties as to the plain meaning of the term, we adopt for purposes of this Decision that the plain and ordinary meaning of the phrases "exception to a security rule" or "exceptions to security rules" mean "an instance in which a security rule does not apply." *See* PO Resp. 8–16; Pet. Reply 2–5; Ex. 2005 ¶¶ 41–57; Ex. 1002 ¶¶ 66, 114–115, 134, 185; Ex. 2006, 62:2–24.

2. Claim 23 - Means Plus Function Limitations

Independent claim 23 is directed to a system and recites a number of means plus function limitations. Ex. 1001, 18:22–37. 35 U.S.C. § 112 "allows a patentee to express a claim limitation by reciting a function to be performed rather than by reciting structure or materials for performing that function." *Northrop Grumman Corp. v. Intel Corp.*, 325 F.3d 1346, 1350 (Fed. Cir. 2003). A term written in means-plus-function form is construed to cover "the corresponding structure, material, or acts described in the specification and equivalents thereof" for performing the recited functions. 35 U.S.C. § 112, para. 6.

Use of the term "means" creates a rebuttable presumption that a claim term is a means-plus-function limitation. *Williamson v. Citrix Online, LLC*, 792 F.3d 1339, 1348 (Fed. Cir. 2015). This presumption may be rebutted if the claim recites structure sufficient to perform the described functions in their entirety. *TriMed, Inc. v. Stryker Corp.*, 514 F.3d 1256, 1259 (Fed. Cir. 2008). "Sufficient structure exists when the claim language specifies the

exact structure that performs the functions in question without need to resort to other portions of the specification or extrinsic evidence for an adequate understanding of the structure." *Id.* at 1259–1260; *see Inventio AG v. ThyssenKrupp Elevator Ams. Corp.*, 649 F.3d 1350, 1357 (Fed. Cir. 2011) (noting that one may still consider the written description to "inform the analysis of whether the claim recites sufficiently definite structure to overcome the presumption that § 112 ¶ 6 governs the construction of the claim") (*overruled on other grounds by Williamson*, 792 F.3d at 1339).

In our Institution Decision, we preliminarily adopted Petitioner's construction of the means-plus-function limitations in the challenged claims. Dec. 15. Each of claim 23's limitations is presumptively written in means-plus-function form, and prior to institution, Patent Owner did not attempt to rebut this presumption and did not point to anything in claim 23's limitations that articulated structure sufficient to perform the described functions in their entirety. *Id.* (citing T*riMed v. Stryker*, 514 F.3d at 1259–1260).

Post institution, Patent Owner agrees the terms should be interpreted under 35 U.S.C. §112 ¶ 6 as means-plus-function terms, that the specification describes appropriate corresponding structure for each of these terms, and that each of these terms is not indefinite. PO Resp. 17 (citing Pet. 18–20; Ex. 1002 ¶¶ 116–133). For some of the claim terms, Patent Owner identifies "a more complete listing of corresponding structure." *Id.*

In its Reply, Petitioner does not object to Patent Owner's identification of corresponding structure. *See generally* Pet. Reply.

a) [23A] means for storing values associated with each of a plurality of vulnerabilities

For limitation [23A], "*means for storing values associated with each of a plurality of vulnerabilities*," Petitioner asserts that "[t]he function is

'storing values associated with each of a plurality of vulnerabilities'" and that "[t]he structure is a database, e.g., 'policy monitoring tools database 340.'" Pet. 18 (citing Ex. 1001, 8:61–9:4 ("After a value has been assigned…network monitoring system 150 may ***store this information in, for example, policy monitoring tools database 340***."); Fig. 3; 4:58–65) (emphasis by Petitioner). Petitioner explains that "[p]olicy monitoring tools database 340 may be implemented on any computer-readable medium accessible by 'network monitoring system 150,' (*id.*, 4:58–65), and information in the database 'may be stored using a data structure that includes multiple links between the individual databases [310-340]'" (*id.*, 6:21–25). Pet. 18 (citing Ex. 1002 ¶¶ 116–118).

In its Response, Patent Owner does not object to Petitioner's identification of the function, but states that the corresponding structure "is a memory, storage device and/or database." PO Resp. 17 (citing Ex. 1001, 1:66–2:1, 4:7–12, 4:14–27, 4:42–57, 4:58–6:26, 6:48–53, 7:29–30, 8:61–9:4, 9:24–27, 9:37–40, 9:43–48, 10:25–31, 12:23–29, 13:21–24, Figs. 1, 2, 3, 5, 6).

Petitioner does not object to Patent Owner's identification of corresponding structure. *See generally* Pet. Reply.

Given the descriptions identified by the parties in the '960 patent and the lack of any meaningful dispute, we apply § 112 ¶ 6 and determine that (1) the recited function is storing values associated with each of a plurality of vulnerabilities; and (2) the corresponding structure is a memory, storage device and/or database such as policy monitoring tools database 340.

b) [23B] means for scanning a network element to identify vulnerabilities, the vulnerabilities representing potential points of attack

For limitation [23B], "*means for scanning a network element to identify vulnerabilities, the vulnerabilities representing potential points of attack*," Petitioner asserts that "[t]he function is 'scanning a network element to identify vulnerabilities, the vulnerabilities representing potential points of attack,'" and "[t]he structure is 'scanner 130.'" Pet. 19 (citing Ex. 1001, 18:25–27; Fig. 1, 2:34–42, 3:18–21 ("Scanner 130 may include one or more scanners used to detect anomalies in network devices."). Petitioner asserts that "[n]etwork monitoring system 150 receives data from scanner 130 to 'facilitate the identification of potential vulnerabilities.'" Pet. 19 (citing Ex. 1001, 3:40–42; Ex. 1002 ¶¶ 119–121).

In its Response, Patent Owner does not object to Petitioner's identification of the function, but states that the corresponding structure "is a scanner or scanning device." PO Resp. 17 (citing Ex. 1001, 2:34–42, 3:18–31, 3:40–48, 9:19–27, 9:41–43, 12:47–60, 14:13–21, and/or Figs. 1, 5 and/or 6).

Petitioner does not object to Patent Owner's identification of corresponding structure. *See generally* Pet. Reply.

Given the descriptions identified by the parties in the '960 patent and the lack of any meaningful dispute, we apply § 112 ¶ 6 and determine that (1) the recited function is scanning a network element to identify vulnerabilities, the vulnerabilities representing potential points of attack; and (2) the corresponding structure is a scanner or scanning device such as scanner 130.

c) [23C] means for identifying at least one of the plurality of vulnerabilities associated with the network element based on output from the means for scanning

For limitation [23C], *means for identifying at least one of the plurality of vulnerabilities associated with the network element based on output from the means for scanning*, Petitioner asserts that "[t]he function is 'identifying at least one of the plurality of vulnerabilities associated with the network element based on output from the means for scanning'" and that "[t]he structure is 'network monitoring system 150.'" Pet. 19 (citing Ex. 1001, 4:2–4 ("Network monitoring system 150 may be used to identify potential vulnerabilities for such attack"); 3:32–48; Fig. 1; 2:34–39). Petitioner asserts that "[n]etwork monitoring system 150 may also include generic computing elements." Pet. 19 (citing Ex. 1001, 4:7–12; Ex. 1002 ¶¶ 122–124).

In its Response, Patent Owner does not object to Petitioner's identification of the function, and states that the corresponding structure "is a network monitoring system." PO Resp. 17–18 (citing Ex. 1001, 2:34–42; 3:32–48, 4:2–12, 4:42–57, 4:62–65, 5:23–30, 7:59–8:13, 12:47–60, 14:13–21, 14:47–58, Figs. 1, 2, 5, 6).

Petitioner does not object to Patent Owner's identification of corresponding structure. *See generally* Pet. Reply.

Given the descriptions identified by the parties in the '960 patent and the lack of any meaningful dispute, we apply § 112 ¶ 6 and determine that (1) the recited function is identifying at least one of the plurality of vulnerabilities associated with the network element based on output from the means for scanning; and (2) the corresponding structure is a network monitoring system such as network monitoring system 150.

d) [23D] means for generating a risk indicator for the network element based on the stored value associated with the at least one identified vulnerability

For limitation [23D], "*means for generating a risk indicator for the network element based on the stored value associated with the at least one identified vulnerability*," Petitioner asserts that "[t]he function is 'generating a risk indicator for the network element based on the stored value associated with the at least one identified vulnerability'" and that "[t]he structure is 'network monitoring system 150.'" Pet. 19–20 (citing Ex. 1001, 9:15–30 ("Network monitoring system 150 may then generate a score for each of the identified network elements")). Petitioner asserts that "[n]etwork monitoring system 150 may also include generic computing elements." Pet. 20 (citing Ex. 1001, 4:7–12; Ex. 1002 ¶¶ 125–127).

In its Response, Patent Owner does not object to Petitioner's identification of the function, and states that the corresponding structure "is a network monitoring system." PO Resp. 18 (citing Ex. 1001, 2:4–8, 2:34–42, 3:32–48, 4:5–12, 4:42–57, 5:43–57, 7:59–8:13, 8:14–9:50, 10:19–10:60, 12:32–13:6, 14:22–64, Figs. 1, 2, 5, 6).

Petitioner does not object to Patent Owner's identification of corresponding structure. *See generally* Pet. Reply.

Given the descriptions identified by the parties in the '960 patent and the lack of any meaningful dispute, we apply § 112 ¶ 6 and determine that (1) the recited function is generating a risk indicator for the network element based on the stored value associated with the at least one identified vulnerability; and (2) the corresponding structure is a network monitoring system such as network monitoring system 150.

e) [23E] means for adjusting the risk indicator, subsequent to generating the risk indicator, based on exceptions to security rules stored in the system

For limitation [23E], "*means for adjusting the risk indicator, subsequent to generating the risk indicator, based on exceptions to security rules stored in the system*," Petitioner asserts that "[t]he function is 'adjusting the risk indicator, subsequent to generating the risk indicator, based on exceptions to security rules stored in the system'" and that "[t]he structure is 'network monitoring system 150.'" Pet. 20 (citing *e.g.*, Ex. 1001, 9:15–10:6 ("network monitoring system 150 may determine whether an exception has been granted . . . If an exception has been granted, network monitoring system 150 may reduce the score associated with this network element.")). Petitioner asserts that "[n]etwork monitoring system 150 may also include generic computing elements." Pet. 20 (citing Ex. 1001, 4:7–12; Ex. 1002 ¶¶ 128–130).

In its Response, Patent Owner Patent Owner does not object to Petitioner's identification of the function, and states that the corresponding structure "is a network monitoring system." PO Resp. 18 (citing Ex. 1001, 2:34–42, 3:32–48, 4:42–65, 5:58–6:16, 7:59–8:13, 9:50–10:60, 12:20–31, 12:47–60, 13:21–26, 14:13–64, Figs. 1, 2, 5, 6).

Petitioner does not object to Patent Owner's identification of corresponding structure. *See generally* Pet. Reply.

Given the descriptions identified by the parties in the '960 patent and the lack of any meaningful dispute, we apply § 112 ¶ 6 and determine that (1) the recited function is adjusting the risk indicator, subsequent to generating the risk indicator, based on exceptions to security rules stored in

the system; and (2) the corresponding structure is a network monitoring system such as network monitoring system 150.

f) [23F] means for outputting the adjusted risk indicator

For limitation [23F], "*means for outputting the adjusted risk indicator*," Petitioner asserts that "[t]he function is 'outputting the adjusted risk indicator'" and that "[t]he structure is 'output device 270.'" Pet. 20 (citing *e.g.*, Ex. 1001, 4:5–12, 4:32–34, Fig. 2). Petitioner asserts that "[o]utput device 270 'may include one or more conventional mechanisms that output information to the operator, including a display, a printer, one or more speakers, etc.'" Pet. 20 (citing Ex. 1001, 4:32–34; Ex. 1002 ¶¶ 131–134).

In its Response, Patent Owner does not object to Petitioner's identification of the function, but states that the corresponding structure "is an output device such as a display, a printer, or speakers." PO Resp. 18 (citing Ex. 1001, 2:34–52, 4:5–12, 4:32–37, 10:61–11:12, 14:13–58, Figs. 1, 2, 4, 5, 6).

Petitioner does not object to Patent Owner's identification of corresponding structure. *See generally* Pet. Reply.

Given the descriptions identified by the parties in the '960 patent and the lack of any meaningful dispute, we apply § 112 ¶ 6 and determine that (1) the recited function is outputting the adjusted risk indicator; and (2) the corresponding structure is an output device such as output device 270 in the form of a display, a printer, or one or more speakers.

D. Prior Art References

1. Andres (Ex. 1003)

Andres is titled "System and Method of Managing Network Security Risks." Ex. 1003, code (54). Andres discloses a security risk management system residing in a computer network environment as illustrated in Figure 1, reproduced below.

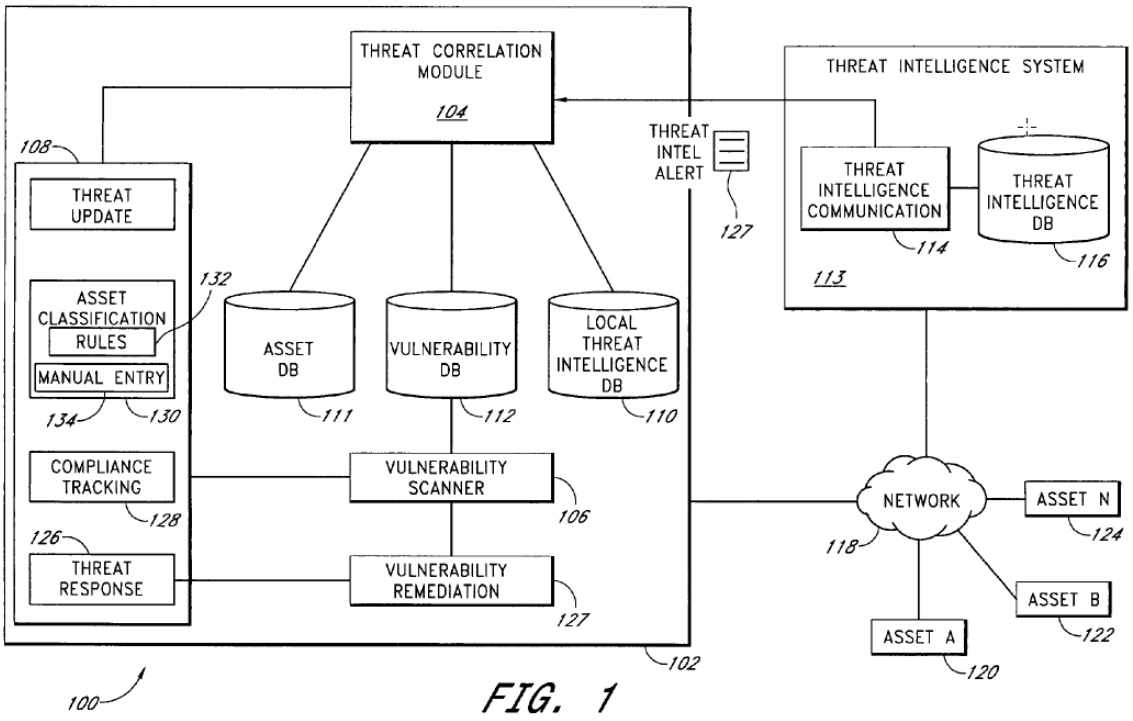
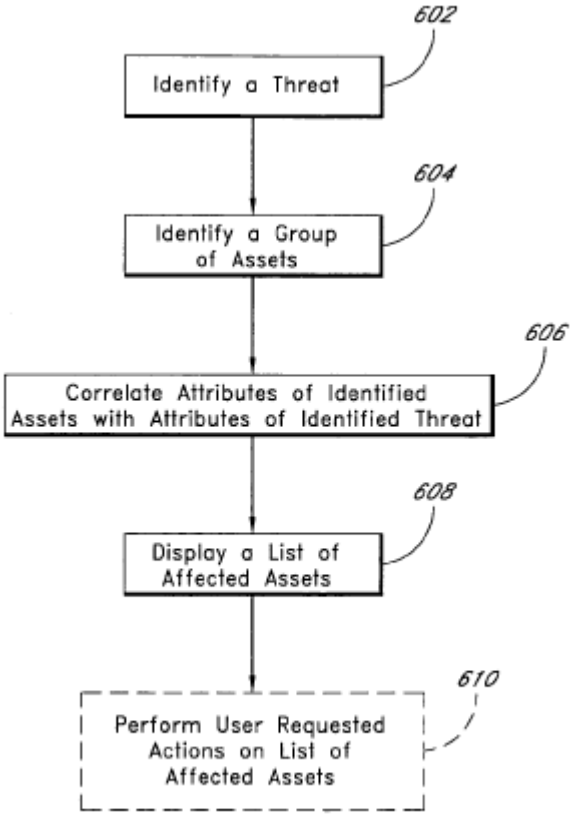


FIG. 1

Andres' Figure 1 is a block diagram of computer network environment 100 including security risk management system 102 connected to assets 120, 122, 124 through communications network 118. *Id.* at 6:3–5, 6:43–46. Security risk management system 102 includes vulnerability scanner 106 which detects vulnerabilities in assets 120, 122, 124. *Id.* at 10:7–12. Security risk management system 102 further includes threat correlation module 104 which determines which, if any, of assets 120, 122, 124 are susceptible to a selected threat. *Id.* at 13:33–36. Threat correlation

module 104 displays a list of affected assets, each with a calculated risk score representing a level of security risk posed by the affected asset to the computer network. *Id.* at 3:31–36, 13:41–49. The risk score is based on the asset's criticality, the threat's criticality, and vulnerability severity values associated with the asset. *Id.* at 14:36–38.

Andres' Figure 6 is shown below.



Andres' Figure 6, is a flowchart illustrating a process of correlating threat attributes with asset attributes performed by threat correlation module 104. Ex. 1003, 21:23–25. In block 602, a threat is identified by a user from a list of threats available for selection derived from a threat intelligence alert. *Id.* at 21:26–29. In block 604, a group of assets to be correlated with the identified threat is identified. *Id.* at 21:30–31. The identified assets may

include those assets that, based on asset attributes and identified threat attributes, may potentially be affected by the identified threat. *Id.* at 21:31–39. The identified assets may also include all assets on the network. *Id.*

In a block 606, the identified assets are correlated with the identified threat. *Id.* at 21:40–41. The correlation may include comparing attributes of the identified assets with attributes of the identified threat. *Id.* at 21: 41–43. Each attribute of an asset that matches an attribute of the threat increases the likelihood that the asset is susceptible to the threat. *Id.* at 21:43–45. Each attribute that is deemed to be susceptible to the threat, either because its attributes exactly match the attributes of the threat, or because its attributes match closely enough to establish a high confidence level of susceptibility, are added to a list of assets that are actually susceptible to the threat. *Id.* at 21:45–50.

In a block 608, the results of the correlation are displayed, and may include a list of assets susceptible to the threat. *Id.* at 21:31–39. The display may include information about each susceptible asset, including, for example, a user-recognizable asset label, a risk level, an IP address, an asset criticality, matched by information, operating system information, a list of vulnerabilities of the asset, and the like. *Id.* at 21:53–58. The list may be sorted such that the assets with the highest risk scores (most risky) are displayed at the top of the list. *Id.* at 21:58–60.

In optional block 610, a user-requested action may be performed on the results of the correlation. *Id.* at 21:61–62. Compliance tracking information may be calculated, or a threat response initiated, such as displaying remediation information to a user, or commencing an automated ticketing and workflow remediation process. *Id.* at 21:62–67. Also, a

request may be sent to a vulnerability scanner for initiating an immediate threat update in order to update the affected assets' attributes. *Id.* at 21:67–22:2.

2. Dodd (Ex. 1004)

Dodd discloses a security auditing system that identifies security vulnerabilities in various elements throughout a network. Ex. 1004 ¶ 23. Dodd's Figure 1 is shown below.

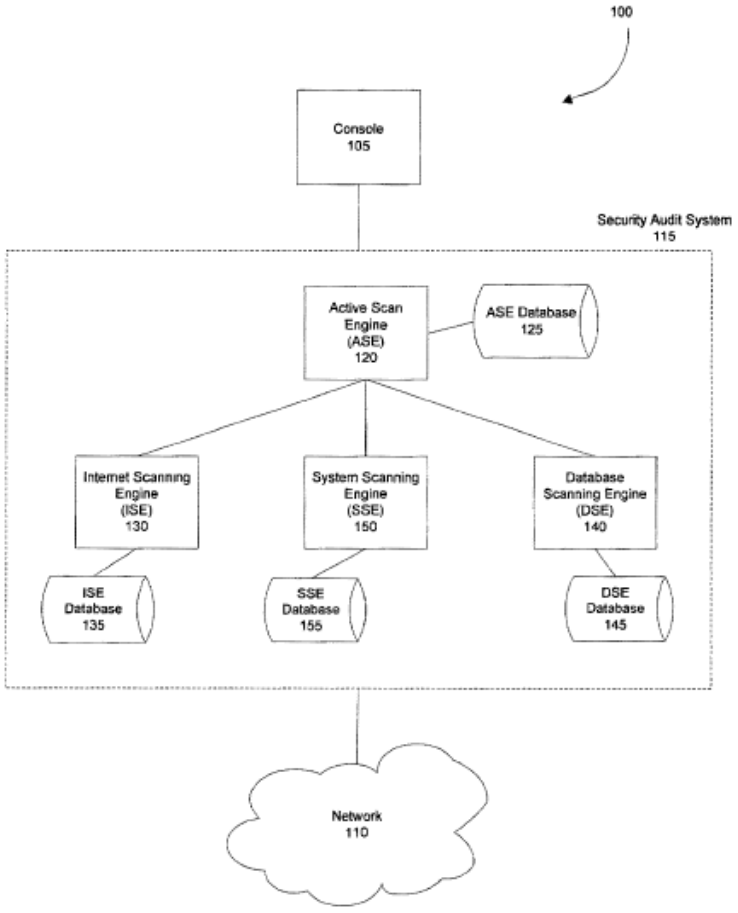


FIG. 1

Dodd's Figure 1 is a block diagram illustrating an exemplary architecture comprising console 105 and security audit system 115 which are used to configure and schedule security audits of network 110. Ex. 1004

¶ 29. Console 105 communicates information about the current security state of network 110 to a user. *Id.* Console 105 is operable for receiving information from security audit system 115 and allowing control of the security audit system 115. *Id.* Security audit system 115 comprises active scan engine 120 and one or more other scan engines. *Id.* Active scan engine 120 is coupled to Internet scanning engine 130, system scanning engine 150, and database scanning engine 140. *Id.* Each scan engine is coupled to a corresponding database. *Id.*

Active scan engine's 120 primary task is acquiring and maintaining current data about the configuration and security posture of network 110. *Id.* ¶ 30. Active scan engine 120 utilizes subsidiary scan engines 130, 140 and 150 as a means for gathering information about network 110. *Id.* Network 110 typically comprises elements such as desktop computers, routers, and various servers. *Id.* Typically, a scan collects information about the function of the hosts on the network and their respective vulnerabilities. *Id.* ¶ 31. This information is gathered, analyzed, and used to compute a security score for each host or element in the network. *Id.* The security scores assist a user or network administrator in determining which vulnerabilities should be addressed first. *Id.*

Active scan engine 120 calculates an asset value for the current host. *Id.* ¶ 32. Asset values are calculated based on the operating system and services associated with the host. *Id.* An asset value is a characteristic representing the importance of a particular host or element in the operation of the network. *Id.* The active scan engine computes a risk value for each vulnerability detected on the current host. *Id.* The risk value quantifies the risk a particular vulnerability presents for a network. *Id.*

Predetermined asset values are generally assigned for the various operating systems, host services, and the vulnerabilities that are likely to be encountered in a scan of a network. *Id.* ¶ 34. These predetermined asset values can be chosen by the provider of the security audit system or the user. *Id.* Respective asset values are retrieved for the host's services and relevant vulnerabilities. *Id.*

Dodd calculates a risk value for each identified security vulnerability based on the asset value, the exploit probability, and the severity value. *Id.* ¶¶ 10, 23. The risk value can be adjusted by a "fix difficulty value" which is a measure of the difficulty of remedying the vulnerability. *Id.* ¶ 37.

Dodd's Figure 5 is shown below.

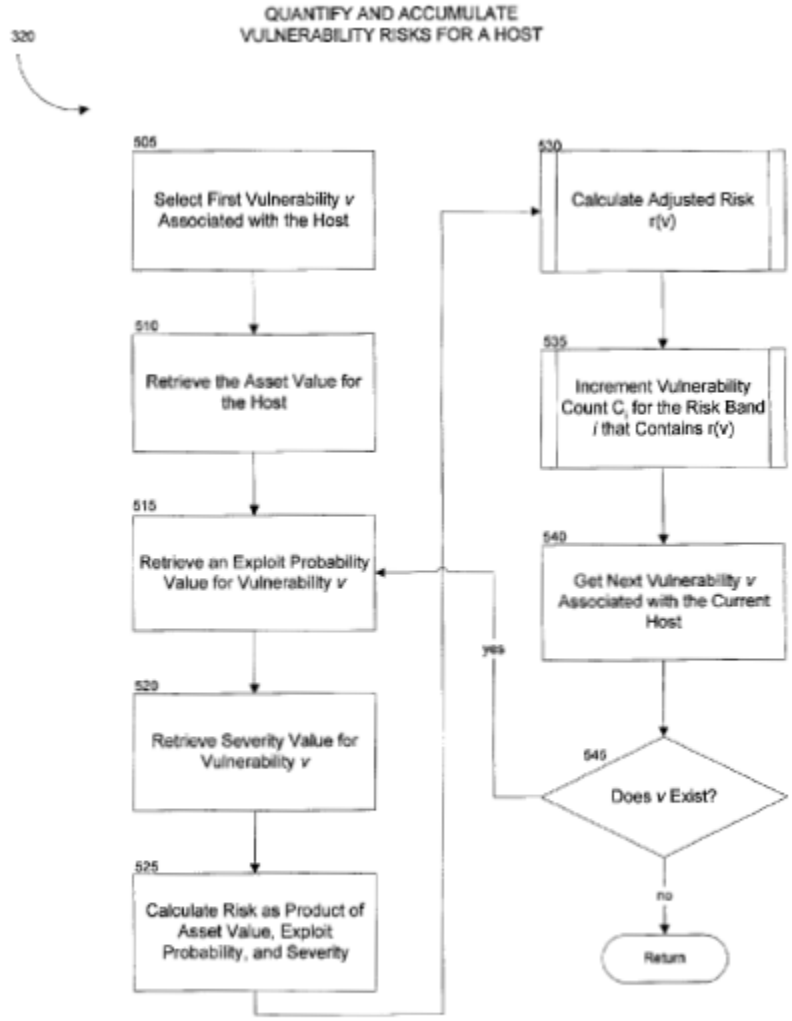


FIG. 5

Dodd's Figure 5 is a logic flow diagram illustrating exemplary process for calculating a risk value for a vulnerability, and for accumulating these risk values for a single host. Ex. 1004 ¶ 16. In step 505 active scan engine 120 selects the first vulnerability discovered on the current host. *Id.* ¶ 35. In step 510, active scan engine 120 retrieves the asset value for the current host. *Id.* Active scan engine 120 retrieves a value representing the probability of a successful exploit against the current vulnerability in step

515. *Id.* Each vulnerability has one or more exploit methods associated with it. *Id.* The likelihood of a successful exploit is related to the difficulty of the exploit method. *Id.* An easily exploited vulnerability is assigned a relatively high exploit probability value. *Id.* To retrieve a vulnerability's exploit probability value, active scan engine 120 first retrieves the vulnerability's exploit method. *Id.* Active scan engine 120 then consults a table that maps exploit methods to probability values. *Id.*

In step 520, active scan engine 120 retrieves a predetermined severity value for the current vulnerability. *Id.* ¶ 36. This value represents the impact of a successful exploit of the vulnerability. *Id.* In step 525, the risk is calculated as the product of the host asset value and the vulnerability' s severity and exploit probability values. *Id.* According to Dodd, alternative embodiments of the present invention may weigh the three factors differently or use less than all three values in calculating the risk value. *Id.* In step 530, active scan engine 120 adjusts the calculated risk value to take into account the difficulty of fixing the current vulnerability. *Id.* The user can choose not to incorporate the fix difficulty factor and instead, use the "pure" risk value. *Id.*

The fix difficulty value is a measure of the difficulty of remedying a vulnerability. *Id.* ¶ 37. Each vulnerability has associated with it one or more fix methods. *Id.* To retrieve a fix difficulty value for a vulnerability, active scan engine 120 first retrieves the vulnerability's fix method. *Id.* Active scan engine 120 then consults a table that maps each fix method to a difficulty value. *Id.* This mapping table is typically created by network security personnel for use by security audit system 115. *Id.* The risk value is multiplied by the fix difficulty value to yield an adjusted risk value. *Id.*

The adjusted risk value for the vulnerability can be compared to other adjusted risk values and ranked from highest to lowest. *Id.* Using this method, when multiple vulnerabilities have the same computed risk, a user of the security audit system can address those that are easier to fix first. *Id.* The adjusted risk value can also be used to calculate the security score so that an element's security score will reflect the difficulty with which its vulnerabilities can be fixed. *Id.*

3. Njemanze (Ex. 1005)

Njemanze discloses a computer-based system that enables aggregation, correlation, detection, and investigative tracking of suspicious network activities. Ex. 1005, 3:27–34. Njemanze's system includes a rules engine used to cross-correlate event data with security rules. *Id.* at 9:54–56. Njemanze describes automatic remediation based on actions triggered by rules. *Id.* at 10:58–63. ("When incoming events match a particular rule's conditions and thresholds . . . the rule automatically fires the action that has been defined."). Njemanze explains that "[t]he actions triggered by the rules may include . . . instructions to network devices . . . to take action to thwart a suspected attack (e.g., by reconfiguring one or more of the network devices, and or modifying or updating access lists, etc.)." *Id.* at 9:66–10:10.

E. Contested Issues

Patent Owner opposes the Petition and raises the following contested issues:

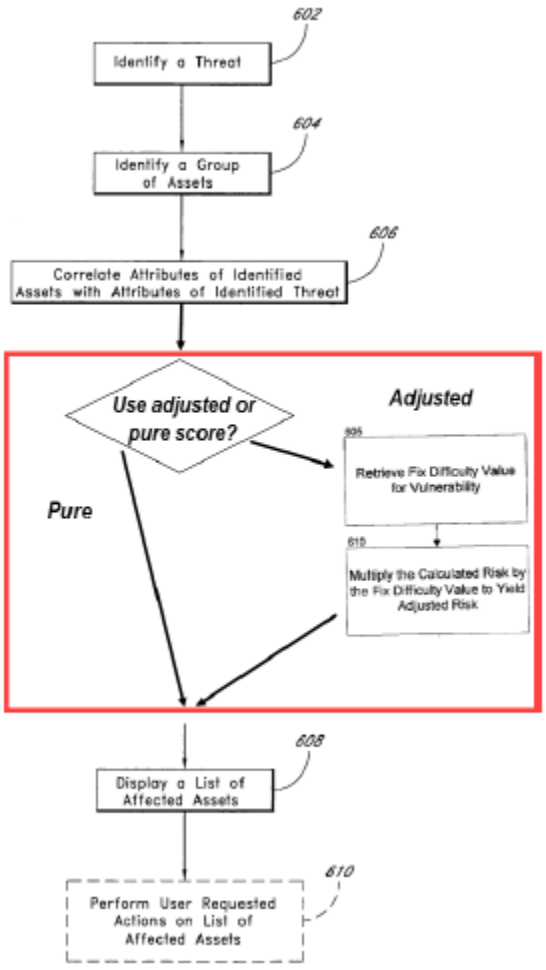
1) Whether a person of ordinary skill in the art ("POSITA") would have had reason to combine Andres and Dodd in the manner proposed by Petitioner (PO Resp 45–55; PO Sur-reply 21–22);

2) Whether Petitioner's proposed combination of Andres/Dodd discloses the recited "exception" limitations, including determining whether an exception "exists" (PO Resp. 23–45; PO Sur-reply 2–21);
3) Whether the Petition properly addresses the "means" limitations of claim 23, including whether Andres/Dodd discloses the recited "means for adjusting . . . based on exceptions to security rules" limitation (PO Resp. 56–57; PO Sur-reply 25–27);
4) Whether Andres/Dodd discloses the recited "automatically performing remedial action" limitation of claim 4 (PO Resp. 57–62; PO Sur-reply 23–24); and
5) Whether Andres/Dodd discloses the recited "quarantining or preventing access" limitation of claim 5 (PO Resp. 57–62; PO Sur-reply 24–25).

We first consider the evidence and the arguments concerning Petitioner's position that a person of ordinary skill in the art would have had reason to combine Andres and Dodd in the manner Petitioner proposes.

1. Rationale to Combine

Petitioner contends that a person of ordinary skill in the art "would have been motivated to combine Andres and Dodd to provide a risk score adjustment process, as taught by Dodd, to Andres's network security risk management system." Pet. 21. Petitioner illustrates the proposed combination using a modified figure, shown below, that "shows Dodd's adjustment process superimposed onto the threat correlation process of Andres's Figure 6." Pet. 21–22 (citing Ex. 1002 ¶¶ 136–137).



Petitioner's combined illustration of Andres and Dodd depicts a portion of Dodd's process for adjusting a vulnerability's calculated risk value (Ex. 1004 ¶ 17; Fig. 6) incorporated into Andres' process of correlating threat attributes with asset attributes performed by the security risk management system (Ex. 1003, 3:64–67; Fig. 6). Pet. 22.

Petitioner argues that a person of ordinary skill in the art "would have been motivated to modify Andres's system in view of Dodd's teachings to provide the option to consider the difficulty in fixing a particular vulnerability." Pet. 22. Petitioner points out that "Andres teaches a

vulnerability remediation module 127 which 'provides automated ticketing and workflow that manages remediation activities' (Ex. 1003, 19:39–41) and that risk scores should inform the remediation process, such that administrators can 'first take the remediation steps that will most significantly improve the overall security of the network.'" Pet. 22–23 (citing Ex. 1003, 18:21–23). Petitioner asserts that "Dodd similarly teaches 'when multiple vulnerabilities have the same computed risk, a user of the security audit system can address those that are easier to fix first.'" Pet. 23 (citing Ex. 1004 ¶ 37). "Such remediation prioritization," Petitioner argues, "allows an administrator to be more effective in his or her responsibilities even with the limited time and resources of many administrators." Pet. 23 (citing Ex. 1003, 18:23–25; Ex. 1002 ¶¶ 138–140).

Petitioner asserts that "Dodd provides the option to use a 'fix difficulty value' for the vulnerability to adjust a risk value associated with that particular vulnerability." Pet. 23 (citing Ex. 1004 ¶ 36). Petitioner asserts that a person of ordinary skill in the art "would have understood Dodd's optional adjustment of risk values based on the vulnerability fix difficulty to be an obvious addition to Andres." Pet. 23. "Indeed," Petitioner argues, "the same problem of effectively prioritizing remediation actions described in Andres underlies the adjustment process of Dodd." *Id.* (citing Ex. 1004 ¶¶ 10, 23; Ex. 1002 ¶¶ 141–142).

Petitioner also argues that a person of ordinary skill in the art "would have been motivated by the common goals of Andres and Dodd (utilizing risk scoring to inform/prioritize vulnerability remediation) to incorporate Dodd's adjustment process into Andres's system." Pet. 24. "By adding Dodd's option to adjust the risk score by a fix difficulty value to Andres's

system," Petitioner argues, "a user of the combined system could more effectively prioritize the easiest to fix vulnerabilities, and therefore decrease the number of vulnerabilities threatening the network." *Id.* (citing Ex. 1004 ¶ 37). "This would facilitate the early resolution of easier vulnerabilities," Petitioner argues, "before they can be exploited in an attack and allow the 'limited time and resources' of administrators to be focused on the more difficult vulnerabilities." *Id.* (citing Ex. 1003, 18:23–25). Petitioner argues that the enhanced prioritization "would also allow administrators to incorporate business factors such as cost into decisions about remediation." *Id.* (citing Ex. 1002 ¶¶ 143–144).

Petitioner also argues that a person of ordinary skill in the art "would have been motivated to add [Dodd's] adjustment processes to Andres's system to fulfill Andres's goal of tailoring the generated risk scores to the needs of the organization." Pet. 24. Petitioner argues that this "would help achieve Andres's goal of enabling users to 'more quickly recognize and attempt to remediate the security flaws found in the assets that are at higher risk and therefore pose a greater security threat to the network as a whole.'" Pet. 24–25 (citing Ex. 1004, 14:30–33; Ex. 1002 ¶ 147).

Petitioner argues that a person of ordinary skill in the art "would have had a reasonable expectation of success in combining Andres with Dodd because the combination would have merely entailed applying Dodd's adjustment processes to the combined system to yield the predictable results of providing an adjustment to the risk score after generation." Pet. 25. Petitioner argues that it "would be a trivial modification of Andres's calculation methods to calculate a 'pure' risk score or to optionally apply Dodd's fix difficulty value to adjust the risk score." Pet. 26. Petitioner

points out that both Andres's and Dodd's methods "include mathematical approaches to quantifying risk and rely on numeric variables representing asset value and vulnerability severity." *Id.* (citing Ex. 1004 ¶ 9; Ex. 1003, claim 3; Ex. 1002 ¶¶ 150–151). Petitioner argues that the Andres/Dodd combination would thus "be the use of known mathematical techniques to improve similar products in the same way." Pet. 26.

Petitioner also argues that a person of ordinary skill in the art "would have understood that Dodd's risk value adjustment procedure is applicable to Andres's risk score" and "[t]he Andres/Dodd combination would have been considered combining prior art elements (Andres's system of risk score calculation with Dodd's adjustment process) according to known methods (adding a new software module or modifying Andres's existing threat correlation module with a new formula) to yield the predictable result of providing an adjusted risk score." Pet. 27–28 (citing Ex. 1002 ¶ 160). Petitioner's assertions are supported by the corroborating testimony of Dr. Houh. *See* Ex. 1002 ¶¶ 136–160.

In its Response, Patent Owner disagrees and contends that "the Petition is highlighting reasons that would have led a [POSITA] to choose Dodd's approach ***instead of*** Andres'". PO Resp. 45 (citing Ex. 2005 ¶ 153). Patent Owner asserts that

> the Petition's lengthy description of overlapping features [of Andres and Dodd] boils down to a demonstration that the references are analogous art. But references being analogous art is merely a ***starting*** point for an obviousness case, not a demonstration of a reason that references would have been combined or that subject matter would have been obvious.

PO Resp. 47 (citing *K-Tec, Inc. v. Vita-Mix Corp.*, 696 F.3d 1364, 1375–76 (Fed. Cir. 2012).

Patent Owner argues that "looking at Andres and Dodd, the two references are similar in large part but differ in a significant respect that is at the heart of both techniques." PO Resp. 48 (citing Ex. 2005 ¶ 158). Patent Owner asserts that "Andres is explicit about its focus . . . [and its] analysis therefore focuses on more objective risk factors." PO Resp. 48–49 (quoting Ex. 1003, 4:64–5:7). These factors, Patent Owner explains

> include each asset's "criticality" value indicating "importance of the asset to the organization that owns the asset." (*Id.*, 5:14-18, 10:41-42.) They also include the "criticality of a threat" that is an evaluation of a "severity of the threat" based on whether "individuals, groups, or automated processes are actively purveying the threat," "the level of damage the threat will cause to affected assets," and "an estimated of the number of assets that have already been affected by the threat."

PO Resp. 49 (quoting Ex. 1003, 7:17–26).

With respect to Dodd, Patent Owner asserts that

> Dodd calculates a risk score and bases that score on "the host asset value and the vulnerability's severity." (Petition, 27; Dodd, ¶0010, ¶0023, ¶¶0035-36.) Dodd goes beyond these shared factors in order to help an administrator understand not only what the highest-risk threats are, but also how to allocate their time to have the most practical impact on security. (*Id.*, ¶0023, ¶0037.) Dodd adds a consideration of "the probability of a successful exploit," where an "easily exploited" vulnerability gets a higher value than ones that are "difficult to exploit and involve a complex attack." (*Id.*, ¶0035.)

PO Resp. 49–50.

Patent Owner argues that "Dodd might therefore be considered to present a more practical view of risk, in which ease of fix and likelihood of a threat being exploited are accounted for alongside the more objective risk calculations. Andres, however, focuses only on those more objective risk calculations." PO Resp. 50.

Patent Owner then argues that a person of ordinary skill in the art

> would have understood that the two references overlap in connection with objective risk analyses like vulnerability severity values and importance of assets. A POSA would have understood that Dodd already represents an extension of Andres' approach and a difference in focus, from a more objective view of risk (as in Andres) to a more practical view of risk (as in Dodd). A POSA would have understood that modifying Andres based on Dodd as proposed by the Petition would not simply be expanding Andres' functionality, but would be more akin to ***turning Andres into Dodd***. If a POSA already had access to Dodd's approach, including the objective risk factors used by Andres and Dodd as well as Dodd's practical risk factors, the record does not support a conclusion that a POSA would have taken up the burden of modifying Andres rather than just choosing Dodd.

PO Resp. 51 (citing Ex. 2005 ¶ 162).

Patent Owner asserts that "[t]he Petition does not provide any sustainable reason that a POSA would have been led to ***combine*** Andres and Dodd instead of choosing between them." PO Resp. 51.

Patent Owner argues that a person of ordinary skill in the art

> would not have found it advantageous to take practical risk factors from Dodd and modify Andres to incorporate those practical risk factors. Instead, a POSA would have been motivated to ***either*** "'first take the remediation steps that will most significantly improve the overall security of the network'" (Andres, 18:21-23) ***or*** prioritize remediation "based on the ease with which the vulnerability can be repaired" (Dodd, ¶0023). Accordingly, what the Petition proposes as a reason to combine the references represents a decision a POSA would have made based on a desired prioritization of information, between objective risk and practical risk. Indeed, if a POSA chose to prioritize vulnerability remediation based on "the ease with which the vulnerability can be repaired" as per Dodd, the POSA would just have chosen Dodd's approach at least in view of the substantial overlap in the references' analyses, rather take the

> material that differentiates the references out of Dodd and put it into Andres.

PO Resp. 52–53 (citing Ex. 2005 ¶ 163).

Patent Owner also disputes that "adding the cited functionality from Dodd would have furthered 'Andres's goal of tailoring the generated risk scores to the needs of the organization.'" PO Resp. 53 (quoting Pet. 24). Patent Owner argues that even though "the Petition cites to Andres' discussion of 'asset criticality' that measures importance of network assets in an organization . . . the Petition here fails to address that Dodd already uses 'asset value' to identify 'the importance of a particular host or element in the operation of the network.'" PO Resp. 53 (citing Pet. 24–25; Ex. 1003, 10:36–38, 10:41–44; Ex. 1004 ¶ 32). Patent Owner argues that "the record does not suggest any reason that Andres' use of asset criticality in calculating its measure of objective risk would have led a POSA to modify Andres to incorporate Dodd's practical risk metrics, such as its fix difficulty value." PO Resp. 54–55 (citing Ex. 2005 ¶ 164).

Patent Owner contends that

> Andres and Dodd represent two techniques for accomplishing the same goal, and provide different perspectives on that goal: one (Andres) measuring objective risk and one (Dodd) adding factors for practical risk on top of those objective risk factors. The two rely on the same metrics to make their determinations, but the practically-focused one (Dodd) adds more metrics. Rather than turn Andres into Dodd through a combination of the references, a POSA would have merely selected between them.

PO Resp. 55 (citing Ex. 2005 ¶ 165).

In its Reply, Petitioner argues that "because Dodd identifies a known problem (e.g., how administrators should allocate their time to have the most practical impact on security) and provides a solution to address the problem

(e.g., adjusting the risk value of each vulnerability to consider a 'fix difficulty value' and prioritizing remediation of vulnerabilities based on the adjusted score)," that this is sufficient to have motivated a person of ordinary skill in the art to combine Andres with Dodd. Pet. Reply 15–16.

Petitioner also argues that "Dodd's use of the fix difficulty value to adjust the risk value of a vulnerability is a 'universal motivation' known in the field of network security and improves the technology, by ensuring that the remediation of the vulnerabilities will consider the fix difficulty value." *Id.* at 16. Petitioner quotes *Intel Corp. v. PACT XPP Schweiz AG*, 61 F.4th 1373, 1381 (Fed. Cir. 2023), for the proposition that "'Universal' motivations known in a particular field to improve technology provide 'a motivation to combine prior art references even absent any hint of suggestion in the references themselves.'" Pet. Reply 16. According to Petitioner, "the ability to use Dodd's fix difficulty value-adjusted score to identify and subsequently remediate security vulnerabilities would directly enhance Andres' goals of 'allow[ing] an administrator to be more effective in his or her responsibilities even with the limited time and resources of many administrators.'" *Id.* at 17 (citing Ex. 1003, 18:23–25; Ex. 1020 ¶ 33).

We agree with Petitioner that a person of ordinary skill in the art would have had sufficient reason to combine the teachings of Andres and Dodd in the manner described in the Petition. Petitioner provides sufficient explanation of how and why a person of ordinary skill in the art would have combined the teachings of Andres and Dodd and has also described in sufficient detail the proffered combination.

In particular, we credit the testimony of Dr. Houh that a person of ordinary skill in the art "would have been motivated to modify Andres's

system in view of Dodd's teachings to provide the option in Andres's system to complement Andres's remediation processes to consider the difficulty in fixing a particular vulnerability." Ex. 1002 ¶ 139. Dr. Houh explains that "Andres already discloses remediation processes. For example, Andres teaches a vulnerability remediation module 127 which 'provides automated ticketing and workflow that manages remediation activities.'" *Id.* (citing Ex. 1003, 19:39–41). "Indeed," Dr. Houh testifies, "Andres teaches that the risk score should inform the remediation process, such that administrators can 'first take the remediation steps that will most significantly improve the overall security of the network.'" Ex. 1002 ¶ 139 (citing Ex. 1003, 18:21–23).

Dr. Houh then explains that

> Dodd shares this goal of prioritizing remediation efforts based on risk scores. As an example, Dodd teaches that "when multiple vulnerabilities have the same computed risk, a user of the security audit system can address those that are easier to fix first." EX1004, [0037]. Such remediation prioritization, as Andres notes, "allows an administrator to be more effective in his or her responsibilities even with the limited time and resources of many administrators."

Ex. 1002 ¶ 140 (citing Ex. 1003, 18:23–25). Dr. Houh then explains that in order to accomplish this, "Dodd provides the option to use a 'fix difficulty value' for the vulnerability to adjust a risk value associated with that particular vulnerability." Ex. 1002 ¶ 141 (citing Ex. 1004 ¶ 36).

Dr. Houh testifies that a person of ordinary skill in the art "would have understood Dodd's optional adjustment of the risk value based on the fix difficulty of a vulnerability to be an obvious addition to Andres. Indeed, the same need to prioritizing remediation actions described in Andres underlies the adjustment process of Dodd." Ex. 1002 ¶ 142. As an example,

Dr. Houh points out that "Dodd explains that 'the risk value can also be adjusted by a factor that reflects the difficulty of remedying the vulnerability,'" and that "[t]his results in a system where vulnerabilities can be prioritized 'based on the ease with which the vulnerability can be repaired," as "[p]rioritizing risk values for a particular network element assists a user or network administrator in deciding which vulnerabilities to address first." *Id*. (citing Ex. 1004 ¶¶ 10, 23).

Dr. Houh testifies, and we agree, that a person of ordinary skill in the art "would have been motivated by this common goal of Andres and Dodd (utilizing risk scoring to inform and prioritize vulnerability remediation) to incorporate the specific adjustment process from Dodd into Andres's system," because [b]y implementing Dodd's option to adjust the risk score by a fix difficulty value to Andres's system and method, a user of the combined system would be able to more effectively prioritize the easiest to fix vulnerabilities," as "[t]his would enable the user to efficiently eliminate vulnerabilities threatening the network." Ex. 1002 ¶ 143 (citing Ex. 1004 ¶ 37).

Dr. Houh points out, and we agree, that by "fixing vulnerabilities before they can be exploited in an attack, the combination of Dodd and Andres would allow the 'limited time and resources' of administrators to be focused on the more difficult vulnerabilities." Ex. 1002 ¶ 144 (citing Ex. 1003, 18:23–25).

Dr. Houh also discusses an additional benefit to adding Dodd's adjustment process to Andres' system. Dr. Houh testifies that a person of ordinary skill in the art "would have been motivated to add [Dodd's] adjustment processes to Andres's system to further Andres's goal of

tailoring the generated risk scores to the needs of the organization." Ex. 1002 ¶ 145. Dr. Houh testifies that "Andres already describes some organization-specific factors that impact the calculated risk score. For example, Andres teaches an asset criticality value described as 'a ranking of the importance of the asset to the organization that owns the asset.'" *Id.* Dr. Houh points out that "Andres explains that this 'asset criticality rank can be highly subjective' and 'can be assigned by a user, such as, for example an administrator.'" *Id.* ¶ 146 (citing Ex. 1003, 10:49–54).

Dr. Houh explains that "Dodd's fix difficulty value is another such organization-specific decision about the prioritization of remediation," and that "Dodd recognizes that a user may want to forego using the adjusted risk value in favor of the pure risk value." Ex. 1002 ¶¶ 146–147 (citing Ex. 1003 ¶ 36). Dr. Houh testifies, and we agree, that by "[i]ncorporating such a choice into Andres, by supporting the generation of a pure risk score in addition to a risk score adjusted based on asset criticality, would help achieve Andres's goal of enabling users to "more quickly recognize and attempt to remediate the security flaws found in the assets that are at higher risk and therefore pose a greater security threat to the network as a whole." Ex. 1002 ¶ 147 (citing Ex. 1003, 14:30–33).

Dr. Houh further testifies that a person of ordinary skill in the art "would have had a reasonable expectation of success in combining Andres with Dodd because the combination would have merely entailed applying the adjustment processes described in Dodd to the combined system to yield the predictable results of providing an adjustment to the risk score after generation." Ex. 1002 ¶ 148. We credit Dr. Houh's testimony that "[t]he combination of Andres and Dodd would have been considered combining

prior art elements (Andres's system of risk score calculation with Dodd's adjustment process) according to known methods (adding a new software module or modifying the existing threat correlation module of Andres with a trivial new formula) to yield the predictable results of providing an adjusted risk score." *Id.* ¶ 160.

We disagree with Patent Owner's argument that "[t]he Petition does not provide any sustainable reason that a POSA would have been led to *combine* Andres and Dodd instead of choosing between them." PO Resp. 51. Providing a "sustainable reason" for combining prior art references is not the test for obviousness. Rather, as Justice Kennedy explained in *KSR*, "*any need or problem known in the field* of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 420 (2007) (emphasis added).

We also find unavailing Patent Owner's arguments that a person of ordinary skill in the art would choose between Andres and Dodd rather than combine them or that a person of ordinary skill in the art would choose Dodd's approach instead of Andres. *See, e.g.*, PO Resp. 45, 51. Rather, we find persuasive Dr. Houh's testimony that a person of ordinary skill in the art

> would have been motivated to combine Andres with Dodd, because Dodd identifies a known problem (e.g., how administrators should allocate their time to have the most practical impact on security) and provides a solution to address the problem (e.g., adjusting the risk value of each vulnerability to consider a "fix difficulty value" and prioritizing remediation of vulnerabilities based on the adjusted score).

Ex. 1020 ¶ 32. We credit Dr. Houh's testimony that "Dodd's use of the fix difficulty value to adjust the risk value of a vulnerability is a motivation known in the field of network security and improves the technology, by ensuring that the remediation of the vulnerabilities will consider the fix difficulty value." *Id.*

Dr. Houh also testifies that Petitioner's "proposed modification would not deprive the system of focusing on the 'more objective risk factors,' if an administrator chooses to do so. The system can choose to use or not the FDVs [fix difficulty values] in the risk score calculation. The proposed modification allows this choice." *Id.* ¶ 33. As Dr. Houh explains, and we agree,

> the Petition's combination does not prevent a network administrator from addressing the vulnerabilities based on the pure score (as taught by unmodified Andres). The proposed combination instead allows the administrator to consider—and then choose—another factor in calculating the risk scores. Andres is explicitly interested in improving the "overall" security of the network, and an administrator would appreciate that the overall security of the network may as well be served by considering how easy or difficult it would be to address a particular vulnerability.

Ex. 1020 ¶ 40 (citing Pet. 23; Ex. 1003, 18:21–23).

For these reasons, we find that Petitioner has demonstrated by a preponderance of the evidence that one of ordinary skill in the art at the time of the claimed invention would have had sufficient reason to combine the teachings of Andres and Dodd in the manner described in the Petition and would have had a reasonable expectation of success in that endeavor.

2. Exception Limitations

Each of the challenged independent claims recite the phrase "exception to a security rule" and/or "exceptions to security rules" (the "exception limitations"). The parties have agreed, and we adopt for purposes of this Decision, that the plain and ordinary meaning of the phrases "exception to a security rule" or "exceptions to security rules" mean "an instance in which a security rule does not apply." *See* Sec. III.C.1. Patent Owner, however, disputes that the Petition's Andres/Dodd combination teaches the exception limitations or that the combination teaches determining whether an exception exists. *See, e.g.*, PO Resp. 23–44.

Independent claim 1 is exemplary and includes the following steps reciting the exception limitations:

> [1C] storing, at the network monitoring system, information representing exceptions to security rules (the "storing step");
>
> [1F] determining, by the network monitoring system and subsequent to the generating a risk indicator, whether an exception to a security rule exists with respect to any of the identified vulnerabilities (the "determining step");
>
> [1G] adjusting, by the network monitoring system, the risk indicator for a first one of the network elements in response to determining that an exception to a security rule exists with respect to an identified vulnerability associated with the first network element (the "adjusting step").

Ex. 1001, 15:17–18, 27–30, 31–35.

a) The Parties' Contentions

With respect to the storing step, limitation [1C], Petitioner asserts that "[t]he fix difficulty values in Andres/Dodd are 'information representing exceptions to security rules.'" Pet. 32. Petitioner explains that "[l]ike the '960 patent's exceptions, the fix difficulty values inform the calculation of

the risk indicator for a given asset." *Id.* (citing Ex. 1004 ¶ 37 ("[T]he risk value is multiplied by the fix difficulty value to yield an adjusted risk value."); *compare* Ex. 1001, 9:60–62 ("If an exception has been granted, network monitoring system 150 may reduce the score associated with this network element."); Ex. 1002 ¶¶ 181–182). According to Petitioner, "[t]he Andres/Dodd fix difficulty values represent exceptions (rules) that also adjust a risk score and guide prioritization of addressing/fixing risks in the same way [as the '960 patent]." Pet. 33. "For example," Petitioner explains, "Dodd describes that 'the adjusted risk value for the vulnerability can be compared to other adjusted risk values and ranked from highest to lowest . . . a user of the security audit system can address those that are easier to fix first.'" Pet. 33 (citing Ex. 1004 ¶ 37).

Petitioner explains that

> a particular vulnerability would not be addressed according to its calculated risk; rather, the decision about when to address the particular vulnerability would depend on the difficulty of fixing it. Therefore, the fix difficulty values represent a rule to prioritize remediation of elements, taking into consideration both the vulnerability and risk posed and the cost of fixing the vulnerability. Applying the fix difficulty value and deprioritizing the remediation of a particular vulnerability is an instance in which a particular security rule to address a vulnerability does not apply, because addressing the vulnerability is pushed back.

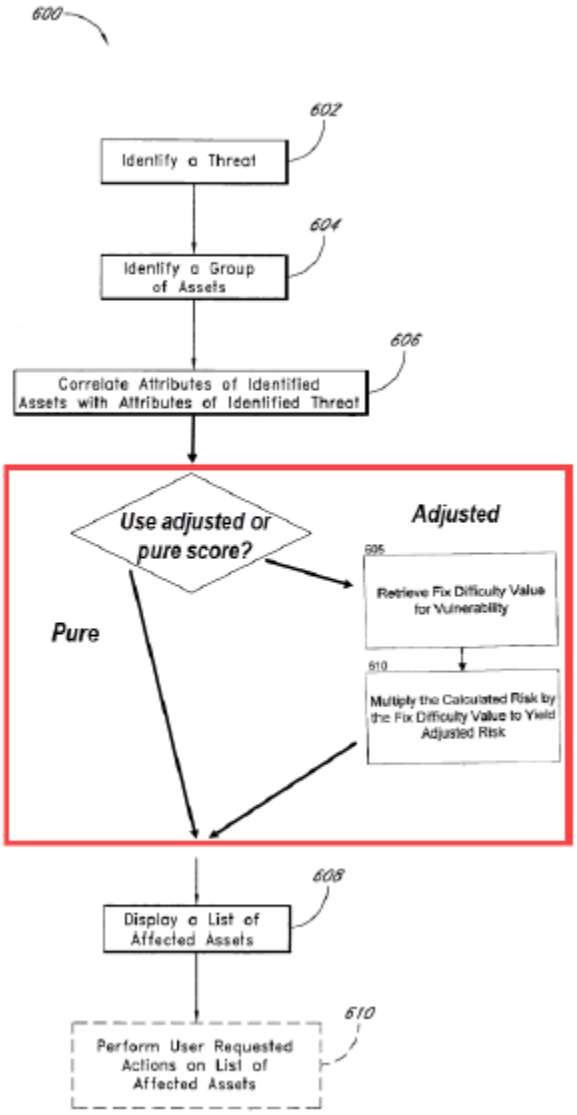
Pet. 33 (citing Ex. 1002 ¶¶ 183–186).

With respect to the determining step, limitation [1F], Petitioner asserts that Andres/Dodd renders this limitation obvious because "[*f*]*irst*, Andres/Dodd renders obvious 'determining, by the network monitoring system . . . whether an exception to a security rule exists with respect to any of the identified vulnerabilities'" as "Andres/Dodd renders obvious storing

information representing exceptions to security rules in the form of the fix difficulty values associated with various vulnerabilities." Pet. 37–38 (citing Pet. at Sec. X.A.2.iv).

Petitioner also points out that "Andres/Dodd teaches that '[i]n step 605, the active scan engine 120 retrieves a fix difficulty value for the vulnerability.'" Pet. 38 (citing Ex. 1004 ¶ 37) (emphasis omitted). According to Petitioner, "Dodd explains that '[*e*]*ach vulnerability* has associated with it one or more *fix methods*' and that 'a table that maps each *fix method* to a *difficulty value*' and that the fix difficulty value 'reflect[s] the difficulty with which its *vulnerabilities* can be fixed.'" Pet. 40 (citing Ex. 1004 ¶ 37; Ex. 1002 ¶ 200).

"*Second*," Petitioner argues, "Andres/Dodd renders obvious that an exception is determined to exist 'subsequent to the generating a risk indicator.'" Pet. 40. Petitioner asserts that a person of ordinary skill in the art "would have implemented the determination that an exception exists after the threat score was calculated, so that the adjusted threat score would indicate which asset to address first and would allow the user to 'first take the remediation steps that will most significantly improve the overall security of the network.'" *Id.* (citing Ex. 1003, 18:21–23). According to Petitioner, "[t]his would provide flexibility to the user to either select a 'pure' risk score or an adjusted risk score." Pet. 40 (citing Ex. 1004 ¶ 36; Ex. 1002 ¶¶ 201–202). To illustrates this, Petitioner provides a modified illustration of Andres' and Dodd's Figure 6, shown below.



Petitioner's modification of Andres' and Dodd's Figure 6 depicts a flowchart that superimposes Dodd's adjustment process (boxed in red) between steps 606 and 608 of Andres process of correlating threat attributes 600. Pet. 41.

With respect to the adjusting step, limitation [1G], Petitioner asserts that "[*f*]*irst*, Andres/Dodd renders obvious 'adjusting, by the network monitoring system, the risk indicator for a first one of the network elements.'" Pet. 42. Petitioner explains that "in the Andres/Dodd system,

fix difficulty values are information representing exceptions to security rules and are determined to exist subsequent to generating the risk indicator." *Id.* (citing Pet. at Secs. X.A.2.v, viii). Petitioner asserts that "[i]n the Andres/Dodd system the fix difficulty values are used to adjust the risk indicator for a network element." Pet. 42. "For example," Petitioner points out, "[i]n step 610, the risk value is multiplied *by the fix difficulty value* to yield an *adjusted risk value*." *Id.* (citing Ex. 1004 ¶ 37; Ex. 1002 ¶¶ 203–204).

Petitioner asserts that "[t]his adjusting is 'by the network monitoring system' because the risk score calculation is done by Andres/Dodd's security risk management system. Pet. 42. "Specifically," Petitioner explains, "the 'threat correlation module 104 allows a user to specify a subset of the network . . . and to calculate an aggregate risk score for the selected subset of assets.'" *Id.* (citing Pet. at Sec. X.A.2.vi; Ex. 1003, 17:58–65, 16:9–15; Ex. 1002 ¶ 205).

"*Second*," Petitioner asserts, "Andres/Dodd renders obvious that this adjustment is "in response to determining that an exception to a security rule exists." Pet. 42. Petitioner explains that "the Andres/Dodd system allows a user to use the fix difficulty value to adjust the risk value." Pet. 43 (citing Pet. at Sec. X.A.1; Ex. 1004 ¶ 36 ("The user can choose not to incorporate the fix difficulty factor and instead, use the 'pure' risk value."). Petitioner points out that Andres's modified Figure 6 incorporates the optional adjustment process of Dodd. Pet. 43 (citing Ex. 1002 ¶ 206).

Petitioner explains that "[i]f a user chooses to incorporate the fix difficulty value, the Andres/Dodd system adjusts the generated risk score. Pet. 45 (citing Ex. 1004 ¶ 37 ("[T]he risk value is multiplied by the fix

difficulty value to yield an adjusted risk value."); Ex. 1002 ¶ 207). According to Petitioner, "[t]he fix difficulty value 'exists with respect to an identified vulnerability associated with the first network element.'" Petitioner points out that "Dodd teaches that the fix difficulty value 'reflect[s] the difficulty with which its *vulnerabilities* can be fixed.'" Pet. 45 (citing Ex. 1004 ¶ 37). Petitioner asserts that "[t]he vulnerabilities are further associated with the network element," as for example, "Dodd teaches how to 'calculate a risk for each *vulnerability associated with an element*.'" Pet. 45 (citing Ex. 1004 ¶ 8; Ex. 1002 ¶ 208).

In its Response, Patent Owner argues that because "[c]laim 1 recites storing 'information representing exceptions to security rules,' as well as subsequently using that exception information in determining whether to adjust a risk indicator," that "[t]he claims thus recite that 'exception' information exists separate and apart from its ***use*** in the claim." PO Resp. 24. Patent Owner asserts that "the Petition does not attempt to argue or cite any information indicating that, ***by themselves***, Dodd's FDVs would have been understood by a [person of ordinary skill in the art] to be information representing exceptions to security rules." *Id.* (citing Ex. 2005 ¶¶ 109–110).

Patent Owner asserts that "Petitioner believes that Dodd's FDVs ***become*** properly interpretable as 'exceptions to security rules' ***upon*** their use in adjusting risk indicators." PO Resp. 26 (citing Pet. 32–33). Patent Owner argues that "[t]his is not enough—the claim language requires ***more*** than adjusting a risk indicator." PO Resp. 26. "For instance," Patent Owner points out, "claim 1 separately recites storing 'information regarding exceptions' and 'determining . . . whether an exception to a security rule exists' ***separate from*** any such adjusting." *Id.*

According to Patent Owner, "the Petition proposes that because Dodd has ***some*** value that is used in ***some*** way to adjust a risk score, that value could have been interpreted to be the claimed 'exception to a security rule.'" *Id.* "Petitioner's interpretation proposal for 'exceptions to a security rule,'" Patent Owner argues, "is thus simply 'a value' that is used in a score adjusting operation." *Id.* at 26–27 (citing Ex. 2005 ¶ 113). "[B]y the Petition's logic," Patent Owner argues, "simply because a value is used in calculating a risk score it should be interpreted as an exception," and "[s]uch a construction cannot be correct because then ***every*** factor used in a calculation of a risk indicator would qualify as 'exceptions to security rules.'" PO Resp. 27.

Patent Owner also argues that the Petition "improperly conflates exceptions and prioritization, two wholly different concepts, both of which are claimed by the '960 patent." PO Resp. 28 (citing Ex. 2005 ¶ 116). Patent Owner argues that there are "at least ***three*** reasons, a [person of ordinary skill in the art] would not have understood prioritization to disclose the exception limitations." PO Resp. 38 (citing Ex. 2005 ¶¶ 137–140). These include: 1) the claim language itself distinguishes between exceptions and prioritization; 2) the Petition itself undermines the allegation that prioritization reads on the exception limitations; and 3) a person of ordinary skill in the art would not have understood mere prioritization to indicate an "exception" to a rule. PO Resp. 39–41.

Patent Owner further argues that "Dodd's FDVs, and their use or non-use in a risk calculation, would not have been understood by a [person of ordinary skill in the art] to be an exception" to a security rule. PO Resp. 30. "Rather," Patent Owner argues, "this would merely represent alternate ways

of calculating a risk score based on more or fewer factors, just like how Dodd describes each of the ***other*** values as optional for its risk calculation." *Id.* (citing Ex. 2004 ¶¶ 119–124). According to Patent Owner, "Dodd explains its FDVs are, like its other vulnerability values (severity and exploit probability), simply a part of the definition of each vulnerability." PO Resp. 32 (citing Ex. 1004 ¶ 37).

Patent Owner indicates that "Dodd further explains that its fix difficulty values are a measure of how difficult it would be to fix a vulnerability," and according to Patent Owner, "[t]he difficulty of fixing a vulnerability is not, of course, any indication of an exception to a security rule." PO Resp. 32–34 (citing Ex. 2005 ¶¶ 127–128, 130). Patent Owner argues that a person of ordinary skill in the art "would not have understood ***any*** of Dodd's vulnerability values (severity, exploit probability, FDV) to be an exception to a security rule." PO Resp. 34 (citing Ex. 2005 ¶ 129).

Patent Owner also argues that a person of ordinary skill in the art "would have understood that, in each case, the decision of whether to use a FDV would be made ***prior to*** any risk calculations and then kept consistent when vulnerabilities are scored within a network, rather than any sort of instance-by-instance decision," and "in any combination of Andres and Dodd, that FDVs would have been used in calculating risk for all vulnerabilities or for no vulnerabilities." PO Resp. 35–36 (citing Ex. 2005 ¶ 134). Patent Owner further argues that "a lower [risk] score by itself does not indicate the presence of an exception or indicate that a security rule does not apply." PO Resp. 36–37.

With respect to "business exceptions," Patent Owner argues that a person of ordinary skill in the art "would not have understood Dodd's FDVs

to be equivalent to or analogous to the '960 patent's 'business exceptions.'" PO Resp. 41–42 (citing Ex. 2005 ¶ 141).

Patent Owner also makes the argument that

> [b]ecause Dodd's FDV is a definitional part of a vulnerability, and because Dodd describes that the FDV is defined for "each" vulnerability, a FDV would always be present in Dodd or Andres-Dodd. Because a FDV exists in every case, there is never a determination of "whether" a FDV "exists" in Dodd or Anders/Dodd. Instead, the value would be known to exist and would simply be retrieved. For the same reason, there is not in Dodd or Andres-Dodd, any adjusting of a risk indicator "in response to determining that an exception to a security rule exists." Instead, since the FDV was known to exist, it would simply be used up on retrieval.

PO Resp. 43 (citing Ex. 2005 ¶ 147).

b) Exceptions to Security Rules

A principal argument in Patent Owner's Response is that Petitioner's asserted prior art, namely the combined Andres/Dodd system, fails to teach the recited "exceptions to security rules." PO Resp. 23–45.

In its Reply, Petitioner asserts that "[Patent Owner's] argument—that Dodd's FDVs cannot meet the requirements of exception to security rules—is based on a fundamental misunderstanding of the Petition." According to Petitioner, "[t]he Petition mapped Dodd's FDVs to the claimed '*information*,' ***not*** to the 'exceptions to security rules.'" Pet. Reply 5–6 (citing Pet. 32–33). Petitioner asserts that "the Petition mapped the 'security rule' to 'prioritizing remediation of vulnerabilities according to ***a pure risk score***.'" Pet. Reply 7 (citing Pet. 33). Whereas, according to Petitioner, "an 'exception to the security rule' is 'prioritizing remediation of vulnerabilities according to ***an adjusted risk score***' (*i.e.*, *which takes into consideration the*

vulnerability and risk posed and the cost of fixing the vulnerability)." *Id.* (citing Pet. at Sec. III.A; D.I. 39).

We agree with Petitioner that Patent Owner misunderstands or misconstrues Petitioner's mapping and that Patent Owner's misunderstanding serves as the basis for many of its arguments. Here, Petitioner's explanation of its mapping is consistent with our preliminary understanding articulated in the Decision on Institution. *See, e.g.*, D.I. 39. In its Reply, Petitioner explains that as discussed in the Petition,

> the Andres/Dodd system generates "***a risk score*** representing a level of security risk posed by the affected asset to a computer network…" Petition, 36 (citing EX1003, 3:31-35). The Petition also noted that "the calculated risk score 214 is based on the asset's criticality, ***the threat's criticality***, and ***vulnerability severity*** values associated with the asset." *Id.,* (citing EX1003, 3:31-35). In the Andres/Dodd system this is a "pure score." *See* Petition, 12-14 (citing EX1004, Figure 5 (step 525); ¶36). ***After*** the pure score has been calculated, the Andres/Dodd system retrieves the FDV for the vulnerability. Petition, 14 (citing EX1004, Figure 6 (step 605)). EX1020, ¶13.
>
> The network administrator then can choose whether or not to incorporate the FDV in the risk score calculation. Petition, 14 (citing EX1004, ¶¶36-37). If the network administrator decides against using the FDV, then the risk score for the particular vulnerability will be the ***pure score***. In this instance, the ***security rule*** would prioritize remediation of the vulnerability according to the ***pure score***. If instead the network administrator decides to use the FDV, then the pure score is adjusted based on the FDV and the risk score for the vulnerability will be the ***adjusted score***. In this instance, ***an exception to the security rule applies***, which would prioritize remediation of the vulnerability according to the ***adjusted score***. For example, the Andres/Dodd system administrator can configure the vulnerability remediation module 127 in a way that is consistent with these security rules and the exceptions. EX1020, ¶14.

Pet. Reply 7–8.

We disagree with Patent Owner's argument that "Petitioner believes that Dodd's FDVs ***become*** properly interpretable as 'exceptions to security rules' ***upon*** their use in adjusting risk indicators." PO Resp. 26 (citing Pet. 32–33). The Petition clearly maps the "fix difficulty values" (FDV) in Andres/Dodd to "*information* representing exceptions to security rules." Pet. 32 (emphasis added). Such information may include, for example, "business exceptions" that may apply to network elements such as those described in the '960 patent. *See, e.g.*, Ex. 1001, 10:13–15. As the Petition explains, the Andres/Dodd fix difficulty values thus "***represent*** exceptions (rules) that also adjust a risk score and guide prioritization of addressing/fixing risks in the same way." Pet. 33 (emphasis added). "Therefore," the Petition explains,

> the fix difficulty values represent a rule to prioritize remediation of elements, taking into consideration both the vulnerability and risk posed and the cost of fixing the vulnerability. Applying the fix difficulty value and deprioritizing the remediation of a particular vulnerability is an instance in which a particular security rule to address a vulnerability does not apply, because addressing the vulnerability is pushed back.

Id. (citing Ex. 1002 ¶¶ 183–186).

We therefore agree with Petitioner that the Petition clearly maps a "security rule" to prioritizing remediation of elements taking into consideration only the vulnerability and risk posed, i.e. a "pure risk score," and "an exception to the security rule" as prioritizing remediation of elements taking into consideration both the vulnerability and risk posed and the cost of fixing the vulnerability, i.e. an "adjusted risk score." Pet. 32–33, 42–43; Pet. Reply 5–7; Ex. 1020 ¶¶ 9–10, 12–14.

We also disagree with Patent Owner's argument that "Petitioner's interpretation proposal for 'exceptions to a security rule' is thus simply 'a value' that is used in a score adjusting operation" and that "[s]uch a construction cannot be correct because then ***every*** factor used in a calculation of a risk indicator would qualify as 'exceptions to security rules.'" PO Resp. 26–27. Patent Owner's argument is based on the misunderstanding that the fix difficulty values can be interpreted to be the claimed exceptions to security rules whereas the Petition makes clear that the fix difficulty values represent a rule to prioritize remediation of elements, taking into consideration both the vulnerability and risk posed and the cost of fixing the vulnerability. *See* Pet 33. Moreover, Patent Owner's argument that "then ***every*** factor used in a calculation of a risk indicator would qualify as 'exceptions to security rules'" is mere unsupported attorney argument and is entitled to little, if any, weight. *See* PO Resp. 26–27. *See Icon Health & Fitness, Inc. v. Strava Inc.*, 849 F.3d 1034, 1046 (Fed. Cir. 2017) ("Attorney argument is not evidence or explanation in support of a conclusion."); *Invitrogen Corp. v. Clontech Lab., Inc.*, 429 F.3d 1052, 1068 (Fed. Cir. 2005) ("Unsubstantiated attorney argument regarding the meaning of technical evidence is no substitute for competent, substantiated expert testimony.").

We also disagree with Patent Owner's argument that "[b]ecause Dodd's FDV is a definitional part of a vulnerability . . . a FDV exists in every case, [and] there is never a determination of 'whether' a FDV 'exists' in Dodd or And[res]/Dodd." PO Resp. 54. Patent Owner's argument fails for two fundamental reasons. First, Petitioner does not equate Dodd's FDV to the recited "determining . . . whether an exception to a security rule

exists" as Patent Owner's argument implies. Rather, Petitioner clearly maps Dodd's FDV to "information representing exceptions to security rules." *See* Pet. 32 ("The fix difficulty values in Andres/Dodd are 'information representing exceptions to security rules.'"). Second, as Petitioner explains, whether Dodd's FDV is used or not depends upon the particular circumstances, because "the fix difficulty value 'reflect[s] the difficulty with which its *vulnerabilities* can be fixed,'" and "the Andres/Dodd system allows a user to use the fix difficulty value to adjust the risk value" or "[t]he user can choose not to incorporate the fix difficulty factor and instead, use the 'pure' risk value." Pet. 40, 43; Ex. 1002 ¶¶ 200, 206; Ex. 1004 ¶¶ 36–37.

With respect to Patent Owner's arguments that the Petition "improperly conflates exceptions and prioritization" (PO Resp. 28), we agree with Petitioner that all three of Patent Owner's arguments "rely on the mistaken assumption that the prior art cannot render obvious the claims because it involves prioritization." Pet. Reply 10. There is no language in the claims that expressly precludes prioritization. *See* Ex. 1001, 15:9–18:37. Indeed, claim 2, which depends from claim 1, expressly recites "prioritizing risk."

First, Petitioner argues, and we agree, that Patent Owner's "claim differentiation argument fails because claim 2 refers to 'prioritizing ***risk***…based on the risk indicators,' e.g., ordering the risk of each vulnerability based on the risk indicators, which ***precedes*** Andres/Dodd's security rule/exception of 'prioritizing ***remediation of elements***,' which is within claim 1's scope." Pet. Reply 10–11.

Second, with respect to Patent Owner's argument that "[n]one of the vulnerabilities, merely by virtue of appearing lower in a prioritized list of vulnerabilities, somehow becomes an 'exception' to a security rule or an instance in which a security rule does not apply," Petitioner asserts, and we agree, that Patent Owner misunderstands Petitioner's argument. Pet. Reply 11. Petitioner asserts that its argument "is that when the remediation of a vulnerability takes the FDV into consideration, this is an exception to the rule that orders the remediation without taking the FDV into consideration." *Id.* "That is," Petitioner explains, "when the FDV is used in the risk score calculation, the remediation of the vulnerability will consider—in addition to the vulnerability and risk posed—the cost of fixing the vulnerability as well." *Id.* (citing Ex. 1020 ¶ 21).

Third, with respect to Patent Owner's argument that a person of ordinary skill in the art would not have understood prioritization to indicate an exception to a rule, Petitioner asserts that Patent Owner "appears to be conflating prioritizing ***risk*** of the vulnerabilities with exceptions, which relate to prioritizing ***remediation*** of the vulnerabilities." Pet. Reply 11–12. We agree with Petitioner and find Patent Owner's argument on this score unavailing.

c) Whether an Exception Exists

Another principal argument in Patent Owner's Response is that the Petition does not demonstrate that an exception to a security rule exists. *See, e.g.*, PO Resp. 25 ("the Petition does not even attempt to demonstrate that there is a 'security rule' and an 'exception' to that security rule"). Patent Owner argues that "claim 1 separately recites storing 'information regarding exceptions' and 'determining . . . whether an exception to a security rule

exists' ***separate from*** any such adjusting," and the Petition does not "attempt to demonstrate that a risk indicator is adjusted in response to determining that such an exception to a security rule exists." PO Resp. 25–26.

Petitioner asserts that Patent Owner is mistaken, and we agree. Pet. Reply 12. Petitioner explains that

> [w]hen the pure score for each vulnerability is calculated, the Andres/Dodd system retrieves the FDV for that vulnerability (EX1004, Figure 6 (step 605)). Dodd discloses that "[t]he user can choose not to incorporate the fix difficulty factor and instead, use the "'pure' risk value." EX1004, ¶36. For example, if the user (network administrator) determines that incorporating the FDV would not change the pure score in a consequential way (e.g., the FDV is "1" or close to "1"), the network administrator could choose to not incorporate the FDV into the risk score calculation. In this case, the administrator determines that there is no exception and therefore the remediation of the vulnerabilities will be prioritized according to the "pure score." But if the difficulties of remedying the vulnerabilities have significant deviations (e.g., FDVs that are much larger/smaller than "1"), then the administrator could choose to incorporate them "to help [the] administrator understand…how to allocate their time to have the most practical impact on security," (EX2005, ¶160) as Dr. Crovella admits. In this case, the network administrator determines that there is an exception to the security rule and therefore the remediation will be prioritized according to the "adjusted score." ***Then*** the system adjusts the pure score, e.g., by multiplying it with the FDV to calculate the "adjusted score." EX1020, ¶24.

Pet. Reply 12–13.

Petitioner further points out that with respect to Patent Owner's argument that "Dodd does not describe, or suggest to a POSA, that this choice would have been made on a per-network element or per-vulnerability basis, or otherwise on an instance-by-instance basis" (PO Resp. 35), that Patent Owner is also mistaken. Pet. Reply 13–14. We agree with Petitioner.

Petitioner points out that "[t]he Andres/Dodd system can choose whether to use the adjusted score or the pure score for each vulnerability of each network element," and that Patent Owner's expert, Dr. Crovella, admitted as much. Pet. Reply 13–14 (citing Ex. 1021, 193:11–18; Ex. 1020 ¶ 26).

Patent Owner argues in its Sur-reply that "both Petitioner and its expert now argue that the 'determining … whether an exception to a security rule exists' is performed on a vulnerability-by vulnerability basis by a '***user (network administrator)*** [who] determines that incorporating the FDV would not change the pure score in a consequential way,'" and that "an act performed mentally/manually by a network administrator is not by a 'network monitoring system' or 'processing device,' so Petitioner's new theory fails to disclose those claim requirements." PO Sur-reply 8–9 (citing Reply 12–13; Ex. 1020 ¶ 24). We disagree with Patent Owner.

Dr. Houh testified, and the Petition's description of the Andres/Dodd system makes clear, that Petitioner is explaining a network administrator's options when configuring the system's rules to codify exceptions an administrator would make when examining a system's vulnerabilities. *See, e.g.*, Ex. 1002 ¶¶ 59 ("It was well known to provide administrative configuration capabilities to override the base scores based on certain rules, thus providing a structured way of adding exceptions," as "[t]hese rules codify exceptions an administrator would make when examining vulnerabilities, **so that the process does not require manual review**.") (emphasis added); Pet. 38 ("The determining is 'by the network monitoring system' because, as shown in Dodd's Figure 1, below, the **active scan engine 120** is part of the **security audit system 115**."), 42 ("This adjusting is 'by the network monitoring system' because the risk score calculation is

done by Andres/Dodd's **security risk management system**. Specifically . . . the 'threat correlation module 104 allows a user to specify a subset of the network . . . and to calculate an aggregate **risk score** for the selected subset of **assets**.'"); Pet. Reply 9 ("These are policies and configurations that can be established by the network administrator to best address the security requirements of the network," and "depending on the policies and configurations established for a particular network, the incorporation of the FDV may adjust the risk score."), 13 ("***Then*** the system adjusts the pure score, e.g., by multiplying it with the FDV to calculate the 'adjusted score.'"). Petitioner's counsel confirmed at the oral hearing that their arguments describe how an administrator makes these adjustments to the system during configuration of the system's rules and policies and that the steps are then performed by the network monitoring system. Tr. 48:14–50:25.

d) Teaching Away

In its Sur-reply, Patent Owner argues that "[t]he references teach away from Petitioner's proposed manual process," and "from Petitioner's proposed vulnerability-by-vulnerability choice of calculations and prioritizations." PO Sur-reply 14–19.

As we discussed above, Patent Owner is mistaken regarding its argument that Petitioner is proposing a "manual" process whereby "a network administrator manually choos[es] to incorporate FDV or not into each individual risk score calculation." PO Sur-reply 14 (citing Pet. Reply 12–14; Ex. 1020 ¶ 24). Dr. Houh testified and the Petition's description of the Andres/Dodd system makes clear, that Petitioner is explaining a network administrator's options when configuring the system's rules to codify

exceptions an administrator would make when examining a system's vulnerabilities. *See* Ex. 1002 ¶¶ 59; Pet. 38, 42; Pet. Reply 9, 13; Tr. 48:14–50:25.

We also disagree with Patent Owner's argument that "[t]he references teach away from Petitioner's proposed vulnerability-by-vulnerability choice of calculations and prioritizations." PO Sur-reply 15 (citing Pet. Reply 14).

In order to "teach away," a reference must actually "criticize, discredit, or otherwise discourage" investigation into the claimed solution. *In re Fulton*, 391 F.3d 1195, 1201 (Fed. Cir. 2004). A reference does not "teach away" if it merely expresses a general preference for an alternative invention from amongst options available to the ordinarily skilled artisan, and the reference does not discredit or discourage investigation into the invention claimed. *Id.* "A reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant. The degree of teaching away will of course depend on the particular facts; in general, a reference will teach away if it suggests that the line of development flowing from the reference's disclosure is unlikely to be productive of the result sought by the applicant." *In re Gurley*, 27 F.3d 551, 553 (Fed. Cir. 1994).

Patent Owner cites to no such disclosures in Andres or Dodd. At best, Patent Owner points to a statement in Dodd of "accurately quantify[ing] the risk posed by vulnerabilities so that they can be compared in association with a particular host and so that hosts can be compared over the entire network." PO Sur-reply, 15. Patent Owner's reference to Andres covers two substantial paragraphs describing, among other things, how "[c]omputer

administrators are responsible for protecting their computer networks from security threats," and "must instead focus on those vulnerabilities that pose the greatest risk to network security" where embodiments of Andres' system "provide tools for manually, semi-automatically, or automatically fixing the vulnerabilities." Ex. 1003, 4:64–5:27. Noting in these disclosures rises to the level of criticizing, discrediting, or otherwise discouraging Patent Owner's proposed system of Andres/Dodd.

Indeed, Dr. Houh testifies that "[i]t was well known to provide administrative configuration capabilities to override the base scores based on certain rules, thus providing a structured way of adding exceptions," and that "[t]hese rules codify exceptions an administrator would make when examining vulnerabilities, so that the process does not require manual review." Ex. 1002 ¶ 59 (citing Ex. 1017, 5). Dr. Houh also testifies that a person of ordinary skill in the art "would have been motivated to modify Andres's system in view of Dodd's teachings to provide the option in Andres's system to complement Andres's remediation processes to consider the difficulty in fixing a particular vulnerability," and that "Dodd shares this goal of prioritizing remediation efforts based on risk scores." Ex. 1002 ¶¶ 139–140. "Such remediation prioritization," Dr. Houh notes, "allows an administrator to be more effective in his or her responsibilities even with the limited time and resources of many administrators." *Id.* ¶ 140 (citing Ex. 1003, 18:23–25).

For these reasons, we find Patent Owner's argument that the references "teach away" from Petitioner's proposed combination of Andres/Dodd to be unavailing.

e) New Theories/Arguments

In its Sur-reply, Patent Owner also asserts that Petitioner's Reply improperly sets out new theories, advances brand-new arguments relying on a new declaration (Ex. 1020) containing opinions not included with the Petition, improperly changes both its claim mapping and its invalidity arguments, and exceeds the proper scope of reply, in particular with respect to the determining step, limitation [1F], and the adjusting step, limitation [1G]. *See* PO Sur-reply 2–7. We disagree with Patent Owner on all scores.

Following institution of trial, our Rules permit a petitioner to file a reply to a patent owner's response and to submit an expert declaration with its reply. *See* CTPG[3] 73 ("A petitioner may file a reply to a patent owner response."). The Board will also "permit the petitioner, in its reply brief, to address issues discussed in the institution decision." *Id.* Although a petitioner "may not submit new evidence or argument in reply that it could have presented earlier," "[a] party also may submit rebuttal evidence in support of its reply." *Id.* (citing *Belden Inc. v. Berk-Tek LLC*, 805 F.3d 1064, 1077–78 (Fed. Cir. 2015)). If a party submits a new expert declaration with its reply, the opposing party may cross-examine the expert, move to exclude the declaration, and comment on the declaration and cross-examination in any sur-reply. *Id.* at 1081–82.

Moreover, parties "are not barred from elaborating on their arguments on issues previously raised" (*Chamberlain Group, Inc. v. One World Techs., Inc.*, 944 F.3d 919, 924–25 (Fed. Cir. 2019)) and reply arguments may be proper where they cite no new evidence and merely expand on or further

[3] *Available at* https://www.uspto.gov/TrialPracticeGuideConsolidated.

explain or clarify previously argued rationales. (*Ericsson Inc. v. Intellectual Ventures I LLC*, 901 F.3d 1374, 1381 (Fed. Cir. 2018)). With respect to Petitioner's reply declaration (Ex. 1020), evidence submitted with an expert declaration filed with petitioner's reply does not violate 37 C.F.R. 42.23(b) where the expert declaration is responsive to patent owner's arguments and patent owner has an opportunity to respond to the evidence. *Belden Inc. v. Berk-Tek LLC*, 805 F.3d 1064, 1078–1080 (Fed. Circ. 2015).

Here, Petitioner's Reply brief and Dr. Houh's Reply Declaration (Ex. 1020) properly respond to and attempt to clarify issues, misunderstandings, arguments, and evidence raised and submitted by Patent Owner in its Response brief and Dr. Crovella's declaration (Ex. 2005). Patent Owner cross-examined Dr. Houh on the testimony in his reply declaration and submitted a transcript of Dr. Houh's deposition into the record. *See* PO Sur-reply, 1; Ex. 2002. We do not discern, nor do we rely upon, any arguments or evidence raised by Petitioner or Dr. Houh that would exceed the proper scope of a reply brief or reply declaration.

The Petition asserts that the proposed combination of Andres/Dodd meets the determining step, limitation [1F], because Andres/Dodd stores "information representing exceptions to security rules in the form of the fixed difficulty values associated with various vulnerabilities." Pet. 37–38. The Petition explains that "Andres/Dodd teaches that '[i]n step 605, the **active scan engine 120** ***retrieves a fix difficulty value*** for the vulnerability.'" *Id.* at 38 (quoting Ex. 1004 ¶ 37). The Petition also explains how Andres/Dodd meets the adjusting step, limitation [1G], explaining that "[i]n step 610, the risk value is multiplied ***by the fix difficulty value*** to yield an ***adjusted risk value***." Pet. 42 (citing Ex. 1004 ¶ 3; Ex. 1002 ¶¶ 203–204).

In his first declaration, Dr. Houh explains how network administrators may make rule adjustments for network monitoring system policies when configuring a system's capabilities. Dr. Houh explains that "[i]t was well known to provide administrative configuration capabilities to override the base scores based on certain rules, thus providing a structured way of adding exceptions." Ex. 1002 ¶ 59. Dr. Houh goes on to explain that "[t]hese rules codify exceptions an administrator would make when examining vulnerabilities, so that the process does not require manual review." *Id.* (citing Ex. 1017, 5).

Petitioner's Reply responds to Patent Owner's argument in its Response that "the Petition does not even attempt to demonstrate that there is a 'security rule' let alone an 'exception' to that security rule." Pet. Reply 7 (quoting PO Resp. 25). As part of its explanation that Patent Owner is mistaken, Petitioner points out that the Petition "noted that 'the calculated risk score 214 is based on the asset's criticality, ***the threat's criticality***, and ***vulnerability severity*** values associated with the asset." Pet. Reply 7–8 (citing Pet. 36; Ex. 1003, 3:31–35). Petitioner's Reply indicates that "[i]n the Andres/Dodd system this is a 'pure score,'" and "[**a**]***fter*** the pure score has been calculated, the Andres/Dodd system retrieves the FDV for the vulnerability." Pet. Reply 8 (citing Pet. 14 (citing Ex. 1004, Fig. 6 (step 605)); Ex. 1020 ¶ 13). Petitioner's Reply states that "[t]he network administrator then can choose whether or not to incorporate the FDV in the risk score calculation." Pet. Reply 8 (citing Pet. 14 (citing Ex. 1004 ¶¶ 36–37)).

Given Dr. Houh's testimony in his first declaration, and the description accompanying the proffered Andres/Dodd system in the Petition,

it is clear to us that in its Reply Brief Petitioner is merely explaining a network administrator's options when configuring the system's rules to codify exceptions an administrator would make when examining a system's vulnerabilities. This understanding is confirmed in the Reply brief where Petitioner explains that "the Andres/Dodd system administrator can configure the vulnerability remediation module 127 in a way that is consistent with these security rules and the exceptions." Pet. Reply 8 (citing Ex. 1020 ¶ 14). Petitioner's Counsel confirmed our understanding of their arguments at the oral hearing in this matter. *See* Tr. 48:14–50:25.

Accordingly, we find Patent Owner's assertions in its Sur-reply that Petitioner's Reply brief sets out new theories, relies on new arguments, improperly changes its claim mapping and invalidity arguments, and exceeds the scope of reply, to be unavailing.

3. Independent Claim 23

In its Response, Patent Owner contends that "the Petition does not meet its burden with respect to demonstrating obviousness of claim 23." PO Resp. 56. Patent Owner asserts that "the Petition merely points to some software code of Andres, such as "scanner 130" or "network monitoring system 150," and "does not identify with particularity a corresponding sequence of acts, which is improper." *Id.* Patent Owner alleges that "the Petition [does not] attempt to map the alleged corresponding structure of the '960 patent to the same or equivalent disclosures in the cited references, as required." *Id.* "Instead," Patent Owner alleges, "the Petition merely cites back to discussion of different language of other claims." *Id.*

In particular, Patent Owner asserts that for limitation [23E], "in connection with 'exceptions to security rules,' the Petition cites solely to

Andres and does not mention Dodd, despite conceding in the rest of the Petition that Andres does not disclose such exceptions." *Id.* at 56–57 (citing Pet. 75; Ex. 2005 ¶¶ 167–170).

Patent Owner contends that "[b]ecause the Petition alleges that language of claim 23 should be interpreted under § 112, ¶ 6, but does not perform a proper obviousness analysis under § 112, ¶ 6, in connection with that language, the Petition's case of invalidity at least in connection with claim 23 is fatally inconsistent and deficient." *Id.* at 57.

In its Reply, Petitioner points out that Patent Owner's Response mistakenly refers to "some software code of Andres, such as 'scanner 130' or 'network monitoring system 150,'" when in fact the Petition refers to structures that are disclosed in the '960 patent. Pet. Reply 22. To show this, Petitioner provides an annotated version of Figure 1 from the '960 patent, shown below.

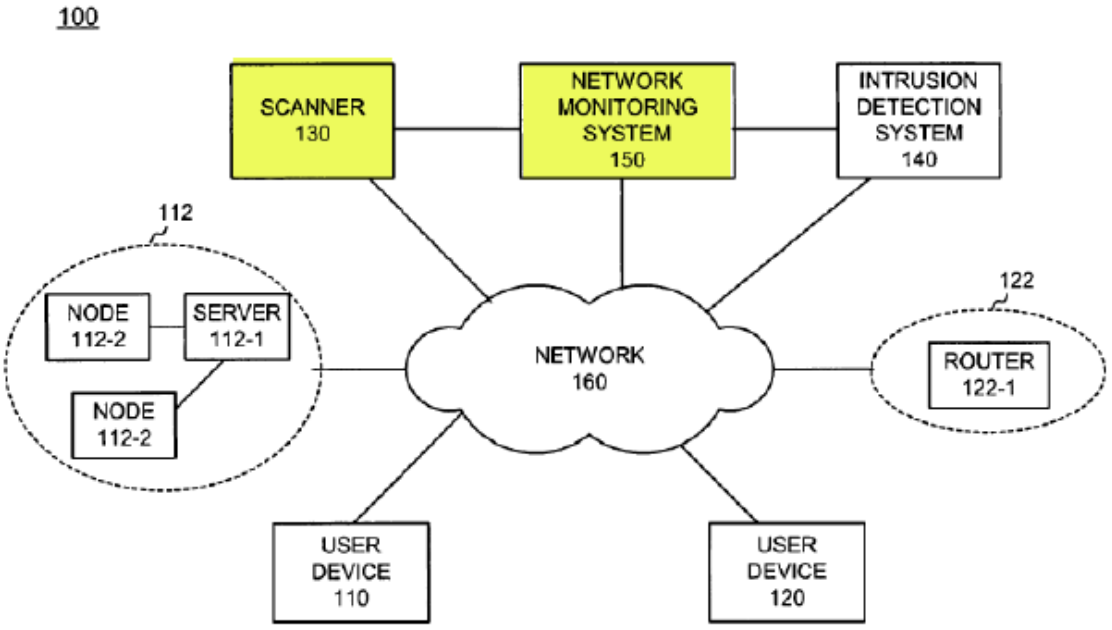


FIG. 1

Petitioner's annotated Figure 1 from the '960 patent is a block diagram depicting system 100 comprising network 160, scanner 130 (in yellow), network monitoring system 150 (in yellow), intrusion detection system 140, domains 112, 122, and user devices 110, 120. Pet. Reply 23. Petitioner contends that the Patent Owner Response "fails to rebut that the identified function/structure in the Andres/Dodd satisfies claim 23." *Id.* (citing Pet. 73–75).

With respect to limitation [23E], Petitioner asserts that Patent Owner mischaracterizes the Petition. *Id.* Petitioner argues that "[t]he Petition identified that the corresponding structure is Andres' 'security risk management system,' but the Petition also pointed to claim 1 and Ex. 1002 ¶¶ 318–319, which discuss how Andres' 'security risk management system' is modified by Dodd's teachings/algorithm to adjust the risk indicators." Pet. Reply 23–24 (citing Ex. 1020 ¶¶ 51–54).

In its Sur-reply Patent Owner disputes Petitioner's arguments and evidence. *See* PO Sur-reply 25–27, including asserting that Patent Owner "presents a new interpretation of 'exceptions to security rules' in which an exception is a different approach to 'prioritizing remediation' than a security rule." PO Sur-reply 26 (citing Pet. Reply 6). Patent Owner argues that Petitioner cannot "demonstrate that its newly-proposed interpretation of "exceptions to security rules" is consonant with the Petition's alleged corresponding structure." PO Sur-reply 26–27.

We now consider Petitioner's showing with respect to claim 23.

a) [Preamble] A system comprising

For the preamble, Petitioner asserts that Andres discloses it. Pet. 73. For support, Petitioner directs us to the Petition, Section X.A.16.i. (claim 18)

and a portion of Dr. Houh's testimony. Pet. 73 (citing Ex. 1002 ¶¶ 308–309). Petitioner identifies Andres' abstract as describing a "security risk management system" and Dr. Houh's corroborating testimony that "Andres discloses a system, specifically a "security risk management system." Pet. 65 (citing Ex. 1002 ¶¶ 279–280).

Based on this evidence, we find that Andres discloses the subject matter described in the preamble of claim 23.

b) [23A] means for storing values associated with each of a plurality of vulnerabilities

For this limitation the recited function is storing values associated with each of a plurality of vulnerabilities and the corresponding structure is a memory, storage device and/or database such as policy monitoring tools database 340. Petitioner asserts that Andres/Dodd renders obvious the same or equivalent structure as "policy monitoring database 340." Pet. 73 (citing Pet. at Sect. X.A.2.iv; Ex. 1002 ¶¶ 310–311).

35 U.S.C. § 312(a)(3) requires that the petition identify, in writing and with particularity, each claim challenged, the grounds on which the challenge to each claim is based, and the evidence that supports the grounds for the challenge to each claim. With respect to limitation [23A], Petitioner has failed to meet that burden.

The problem here is that Petitioner does not actually identify what particular structure in Andres/Dodd is acting as, or is the equivalent of, the identified structure of a "memory, storage device, and/or database such as policy monitoring tools database 340." Without this identification, we are left guessing what structure in Andres/Dodd Petitioner believes satisfies the applicable limitation.

At best, Dr. Houh explains that

> A POSITA would have understood that the fix difficulty values would be stored in the **network monitoring system**, because they would need to be retrieved for the calculation of the adjusted risk score. For example, in the Andres/Dodd system the active scan engine 120 "consults a table that maps each fix method to a difficulty value."

Ex. 1002 ¶ 180 (citing Ex. 1004 ¶ 37).

But here, neither Petitioner nor Dr. Houh identifies where or what in the Andres/Dodd "network monitoring system" stores the fix difficulty values, and the active scan engine 120 mentioned by Dr. Houh is not identified or described as satisfying the identified structure and function of limitation [23A]. Pet. 18, 32–33, 73; Ex. 1002 ¶¶ 116–118, 178–180, 310–311. Petitioner never attempts to identify or explain how any particular structure in Andres/Dodd satisfies both the identified structure of a memory, storage device and/or database such as policy monitoring tools database 340 and the identified function of storing values associated with each of a plurality of vulnerabilities.

We find that Petitioner has not adequately identified a corresponding structure/function in Andres/Dodd that meets the recited limitation [23A], "*means for storing values associated with each of a plurality of vulnerabilities*," identified as a storage device and/or database such as policy monitoring tools database 340 that stores values associated with each of a plurality of vulnerabilities.

Because we find that Petitioner has not shown that Andres/Dodd satisfies limitation [23A], we do not reach the other limitations of claim 23.

4. Dependent Claim 4

Claim 4 depends from claim 3 and recites,

> 4. The method of claim 3, further comprising:

> automatically performing a remedial action with respect to the first network element upon determining that action is required.

Claim 3 depends from claim 1 and recites,

> 3. The method of claim 1, further comprising:
> determining whether action is required with respect to a first one of the network elements based on the risk indicator associated with the first network element.

With respect to claim 4, Petitioner asserts that "Andres discloses this limitation." "For example," Petitioner argues, "Andres teaches that the risk management system 'provide[s] tools for manually, semi-automatically, or ***automatically fixing the vulnerabilities***." Pet. 51 (citing Ex. 1003, 5:23–24). "These tools," Petitioner explains, "include the threat response module 126 and coupled 'vulnerability remediation module 127 [that] provides ***automated ticketing and workflow that manages remediation activities***.'" Pet. 51 (citing Ex. 1003, 19:39–41; Ex. 1002 ¶¶ 226–227).

In its Response, Patent Owner argues that "Andres ***mentions*** automatic fixing, but does not provide any single example or even minimal explanation of how automatically fixing might be implemented," and that "[a] reference including merely two words ('automatically fixing') is not enough to have rendered the claimed subject matter obvious" to a [person of ordinary skill in the art]." PO Resp. 58. Patent Owner argues that "[t]his is particularly the case . . . where the subject matter at issue . . . is complex, and even more so when the technology is complex and the level of ordinary skill in the art is low, as is the case here." *Id.* (citing *OSI Pharm., LLC v. Apotex Inc.*, 939 F.3d 1375, 1385, (Fed. Cir. 2019)). *Id.* Patent Owner argues that because "the Petition does not offer any reference that would

have disclosed to a [person of ordinary skill in the art] how to implement the "automatically performing" of claim 4, claim 4 should be confirmed as not proven unpatentable." PO Resp. 59 (citing Ex. 2005 ¶176).

In its Reply, Petitioner points out, and we agree, that "both Andres and the '960 Patent provide equivalent disclosures about "automatically performing a remedial action." Pet. Reply 24 (citing Ex. 2002, 83:19–22; *compare* Ex. 1003, 19:39–46 *with* Ex. 1001, 11:46–49; Ex. 1020 ¶ 56). Indeed, the '960 patent repeatedly uses the term "automatically" when discussing remediation without explaining in any particular detail how to "automatically" implement the recommended action. *See, e.g.*, Ex. 1001, 11:41–43 ("network monitoring system 150 may take actions to automatically quarantine server 112-1"), 11:47–49 ("network monitoring system 150 may automatically take actions to limit or prevent an attack based on predetermined procedures").

Patent Owner's expert, Dr. Crovella, testified that, in addition to satisfying claims 1 and 3, "[c]laim 4 simply requires . . . that the remedial action is performed automatically." Ex. 1021, 171:15–20. Dr. Crovella also testified that "[t]here is nothing in Claim 4 that limits how it could be implemented." *Id.* at 172:20–21.

Dr. Houh testifies that Andres provides an example of how automatically fixing might be implemented. "For example," Dr. Houh testifies, "Andres provides a 'threat response module may also be configured to access a vulnerability remediation module and initiate an automated ticketing and workflow process that at least partially directs remediation of asset vulnerabilities." Ex. 1020 ¶ 56 (citing Ex. 1003, 2:35–39; 19:39–41).

It is instructive to remember that "[a] person of ordinary skill [in the art] is also a person of ordinary creativity, not an automaton." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 421 (2007). Here, a person of ordinary skill in the art "would have been someone knowledgeable in information technology and networking" and "would have a bachelor's degree in electrical engineering, computer science, or equivalent training, and approximately 2 years of experience working in information technology and networking." *See* Sec. III.B.

Given this evidence, including the level of ordinary skill in the art, the relatively similar uses of the term "automatically" in the '960 patent and Andres, we find that Andres' disclosure of a threat response module that may be configured to access a vulnerability remediation module and initiate an automated ticketing and workflow process that at least partially directs remediation of asset vulnerabilities meets the recited "automatically performing a remedial action," of claim 4.

5. Dependent Claim 5

Claim 5 depends from claim 4 and recites,

> 5. The method of claim 4, where the remedial action comprises:
>
> quarantining or preventing access to the first network element.

With respect to claim 5, Petitioner asserts that "Andres/Dodd/Njemanze renders obvious this limitation." Pet. 82. According to Petitioner, "Njemanze teaches rules that can automatically trigger actions based on network security events." *Id.* "When incoming events match a particular rule's conditions and thresholds . . . the rule automatically fires the action that has been defined." *Id.* (citing Ex. 1005,

10:60–63; Ex. 1002 ¶¶ 334–335). Petitioner asserts that "Njemanze teaches that '[t]he actions triggered by the rules may include . . . instructions to network devices . . . to take action to thwart a suspected attack (e.g., by reconfiguring one or more of the network devices, and or ***modifying or updating access lists***, etc.)." Pet. 82 (citing Ex. 1005, 9:66–10:10).

According to Petitioner, a person of ordinary skill in the art "would have understood that a rule updating the access list for a network device would include preventing access entirely. It was understood that access lists controlled whether devices could receive network traffic." Pet. 82 (citing Ex. 1011, 1:28–30) ("the router may use an ***access list*** that provides conditions or rules to determine whether the packet has access to the particular destination"). Pet. 82 (citing Ex. 1002 ¶ 336).

In its Response, Patent Owner argues that "[a]t best, the record shows that access lists exist and control access, and ***not*** that in the context of Njemanze or the proposed combination with Andres and Dodd that such modifications/updates would include "preventing access entirely." PO Resp. 60 (citing Ex. 2005 ¶ 178). Patent Owner argues that "a clearer record is needed to conclude that a [person of ordinary skill in the art] would have understood ***Njemanze's*** modifications/updates to include the type of "preventing access entirely" that the Petition chooses to try to prove." PO Resp. 61. Patent Owner contends that "Petitioner's expert was evasive when asked to identify whether any reference of record 'explicitly' showed modifying/updating an access list to 'prevent access entirely.'" PO Resp. 61 (citing Ex. 2002, 88:25–114:24; Ex. 2005 ¶ 179).

We disagree with Patent Owner and find its arguments unavailing. First, whether the prior art "explicitly" shows a recited claim term is not the

test for obviousness. Rather, a claim is unpatentable as obvious if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious to a person having ordinary skill in the art to which said subject matter pertains. 35 U.S.C. § 103.

Second, claim 5 does not recite the phrase "prevent access entirely" as Patent Owner implies. Rather, claim 5 recites "quarantining or preventing access to the first network element." Ex. 1001, 15:51–54. Claim terms are generally given their ordinary and customary meaning as understood by a person of ordinary skill in the art in question at the time of the invention. *Phillips*, 415 F.3d at 1313. Importantly, the person of ordinary skill in the art is deemed to read the claim term not only in the context of the particular claim in which the term appears, but also in the context of the entire patent, including the specification. *Multiform Desiccants, Inc. v. Medzam, Ltd.*, 133 F.3d 1473, 1477 (Fed. Cir. 1998); *Phillips* at 1313; *See also Medrad, Inc. v. MRI Devices Corp.*, 401 F.3d 1313, 1319 (Fed.Cir.2005) ("We cannot look at the ordinary meaning of the term . . . in a vacuum. Rather, we must look at the ordinary meaning in the context of the written description and the prosecution history.").

Here, the '960 patent specification uses the terms "quarantining or preventing access" on several occasions, and because a person of ordinary skill in the art is deemed to read claim terms in the context of the entire patent, including the specification, considering how the '960 patent uses these terms can provide insight into how a person of ordinary skill in the art would understand the ordinary and customary meaning of these terms.

For example, the '960 patent explains that "if the risk is high enough, network monitoring system 150 may take actions to automatically quarantine server 112-1 to limit or halt traffic to/from server 112-1." Ex. 1001, 11:41–44. The '960 patent also explains that "network monitoring system 150 may automatically quarantine the vulnerable network element by, for example, shutting down the network element and/or preventing access to the network element by any outside traffic." *Id.* at 12:16–19. Another example from the '960 patent includes " [n]etwork monitoring system 150 may also perform a quarantine action to isolate or limit access to the network element." 13:39–41. These examples do not use the terms "quarantining or preventing access" in such a way that a person of ordinary skill in the art would understand that the ordinary and customary meaning of the terms is "preventing access entirely" as Patent Owner argues. Rather, the '960 patent suggests that the terms "quarantining or preventing access" would encompass limiting traffic to/from a server, preventing access by outside traffic, or limiting access to a network element, none of which are commensurate with "prevent[ing] access entirely," as Patent Owner argues.

For these reasons, we find that Andres' disclosure of actions triggered by rules that may include instructions to network devices to take action to thwart a suspected attack by reconfiguring one or more of the network devices, and or modifying or updating access lists, etc., meets the recited "quarantining or preventing access to the first network element" of claim 5.

F. Obviousness Based on Andres and Dodd (Grounds 1 and 3)

In Ground 1, Petitioner contends that claims 1–4, 7–12, 14–20, 22, and 23 would have been obvious over the combined teachings of Andres and Dodd. Pet. 21. Petitioner provides an analysis as to how the combined

teachings of Andres and Dodd meet the limitations of these challenged claims. Pet. 21–75. Petitioner also provides an explanation as to how and why a person of ordinary skill in the art would have combined the teachings of Andres and Dodd. *Id.* at 21–28. Petitioner relies upon the testimony of Dr. Houh to support its contentions. *See* Ex. 1002 ¶¶ 136–321; Ex. 1020 ¶¶ 6–56, 61–65.

For Ground 3, Petitioner challenges the same claims, but instead uses "Rakuten's claim interpretations, as laid out in Rakuten's Initial Infringement Contentions ('EX1007') in the related litigation." Pet. 21, 85–88; Ex. 1007. Petitioner relies upon the testimony of Dr. Houh to support these contentions. *See* Ex. 1002 ¶¶ 136–160, 349–356.

Patent Owner contends that Petitioner's proposed combination of prior art does not render all of the challenged claims obvious. *See* PO Resp. 19–62. We have considered Patent Owner's evidence and arguments with respect to these disputed issues in Section III.E., *supra*.

With respect to the claims and issues that are not specifically challenged or disputed by Patent Owner, we have reviewed the relevant evidence and arguments of record, including the applicable testimony of Drs. Houh and Crovella.

Upon consideration of the entire record, we determine that Petitioner has shown by a preponderance of the evidence that the combined teachings of Andres and Dodd meet the limitations of claims 1–4, 7–12, 14–20, and 22, and that a person of ordinary skill in the art would have had sufficient rationale to combine their teachings in the manner described by Petitioner and would have had a reasonable expectation of success in so doing.

However, with respect to independent claim 23, we determine that Petitioner has not shown by a preponderance of the evidence that the combined teachings of Andres and Dodd meet the limitations of claim 23.

G. Obviousness Based on Andres, Dodd, and Njemanze (Grounds 2 and 4)

Petitioner contends that claims 2, 5, 13, and 21 would have been obvious over the combined teachings of Andres, Dodd, and Njemanze. Pet. 21, 75–88. Petitioner provides explanations as to how the combination of Andres, Dodd, and Njemanze teaches each claim limitation as well as the rationale for combining the art in the manner proffered. *Id*. Petitioner also relies on the testimony of Dr. Houh to support these contentions. *See* Ex. 1002 ¶¶ 322–356; Ex. 1020 ¶¶ 57–60.

For Ground 4, Petitioner challenges the same claims, but uses "Rakuten's claim interpretations, as laid out in Rakuten's Initial Infringement Contentions ('EX1007') in the related litigation." Pet. 21, 85–88; Ex. 1007. Petitioner relies upon the testimony of Dr. Houh to support these contentions. *See* Ex. 1002 ¶¶ 349–356.

Patent Owner only disputes Petitioner's showing as to dependent claim 5, which we analyze in Section III.E.5.

We have considered all the evidence of record with respect to claims 2, 5, 13, and 21, and determine that Petitioner has demonstrated by a preponderance of the evidence that the proposed combination of Andres/Dodd/Njemanze meets the limitations of claims 2, 5, 13, and 21 and that a person of ordinary skill in the art would have had sufficient rationale to combine their teachings in the manner described by Petitioner and would have had a reasonable expectation of success in so doing.

IV. CONCLUSION

For the foregoing reasons, we determine that Petitioner has demonstrated by a preponderance of the evidence that claims 1–5 and 7–22 of U.S. Patent 7,962,960 B2 are unpatentable on the bases set forth in the following table.[4]

Claims Challenged	35 U.S.C. §	References	Claims Shown Unpatentable	Claims Not Shown Unpatentable
1–4, 7–12, 14–20, 22, 23	103(a)	Andres, Dodd	1–4, 7–12, 14–20, 22	23
2, 5, 13, 21	103(a)	Andres, Dodd, Njemanze	2, 5, 13, 21	

V. ORDER

Upon consideration of the foregoing, it is

ORDERED that Petitioner has demonstrated by a preponderance of the evidence that claims 1–5 and 7–22 of U.S. Patent 7,962,960 B2 are unpatentable;

[4] Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this Final Decision, we draw Patent Owner's attention to the April 2019 *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding. See* 84 Fed. Reg. 16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. *See* 37 C.F.R. § 42.8(a)(3), (b)(2).

FURTHER ORDERED that Petitioner has not demonstrated by a preponderance of the evidence that claim 23 of U.S. Patent 7,962,960 B2 is unpatentable; and

FURTHER ORDERED that because this is a Final Written Decision, any party to the proceeding seeking judicial review of this Decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

For PETITIONER:

Theodoros Konstantakopoulos
Yung-Hoon Ha
DESMARAIS LLP
tkonstantakopoulos@desmaraisllp.com
yha@desmaraisllp.com

For PATENT OWNER:

Heath Briggs
Joshua Raskin
Vimal Kapadia
Andrew Tibbetts
GREENBERG TRAURIG, LLP
briggsh@gtlaw.com
raskinj@gtlaw.com
kapadiav@gtlaw.com
andrew.tibbetts@gtlaw.com