

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC. and FORTINET, INC.,
Petitioner,

v.

INFOEXPRESS INC.,
Patent Owner.

IPR2024-00677
Patent 8,578,444 B2

Before CHRISTOPHER M. KAISER, JOHN A. HUDALLA, and
AARON W. MOORE, *Administrative Patent Judges*.

HUDALLA, *Administrative Patent Judge*.

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314

Cisco Systems, Inc. and Fortinet, Inc. (collectively, “Petitioner”) filed a Petition (Paper 1, “Pet.”) requesting an *inter partes* review of claims 1–7, 10, 12, 17, and 22 (“the challenged claims”) of U.S. Patent No. 8,578,444 B2 (Ex. 1201, “the ’444 patent”). Petitioner filed a Declaration of Henry Houh, Ph.D. (Ex. 1203) with its Petition. InfoExpress, Inc. (“Patent Owner”) filed a Preliminary Response (Paper 7¹, “Prelim. Resp.”), along with declarations of Dr. Eric Cole (Ex. 2001) and Hugh Smith, Ph.D. (Ex. 2007). With our authorization (Paper 9), Petitioner also filed a Preliminary Reply (Paper 11, “Pet. Prelim. Reply”) and Patent Owner filed a Preliminary Sur-reply (Paper 12, “PO Prelim. Sur-reply”) directed to Patent Owner’s attempt to antedate the asserted references.

We have authority to determine whether to institute an *inter partes* review. *See* 35 U.S.C. § 314 (2018); 37 C.F.R. § 42.4(a) (2023). Under 35 U.S.C. § 314(a), we may not authorize an *inter partes* review unless the information in the petition and the preliminary response “shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” For the reasons that follow, we institute an *inter partes* review as to claims 1–7, 10, 12, 17, and 22 of the ’444 patent on the ground of unpatentability presented.

¹ Paper 7 was filed with its availability restricted to “Filing Party and Board.” Patent Owner filed a public version of the Preliminary Response as Paper 8.

I. BACKGROUND

A. *Real Parties-in-Interest*

Petitioner identifies Cisco Systems, Inc. and Fortinet, Inc. as the real parties-in-interest. Pet. 1. Patent Owner identifies InfoExpress Inc. as the real party-in-interest. Paper 5, 1 (Patent Owner’s Mandatory Notices).

B. *Related Matters*

As required by 37 C.F.R. § 42.8(b)(2), the parties identify the following district court cases as related matters:

InfoExpress Inc. v. Fortinet, Inc., No. 4:23-cv-04389 (N.D. Cal. filed Aug. 25, 2023); and

InfoExpress Inc. v. Cisco Systems, Inc., No. 4:23-cv-02698 (N.D. Cal. filed May 31, 2023).

Pet. 1; Paper 5, 1. Patent Owner additionally identifies the following *inter partes* review proceedings as being related: IPR2024-00539, IPR2024-00540, IPR2024-00676, and IPR2024-00678. Paper 5, 1–2

C. *The ’444 Patent*

The ’444 patent is titled “Systems and Methods of Controlling Network Access” and is directed to “[a] new approach to network security.” Ex. 1201, codes (54), (57). The ’444 patent describes “[s]everal approaches to controlling external access to computing networks” that serve the goals of “limiting access to authorized users and assuring that computing devices employed by these users do not include malicious computing code.” *Id.* at 1:29–34. “A first level of access control is achieved by requiring authentication of a user.” *Id.* at 1:38–39. “A greater level of access control may be achieved by including a gatekeeper between the secure network and

the access device.” *Id.* at 1:60–62. Figure 1 of the ’444 patent depicts such a gatekeeper and is reproduced below.

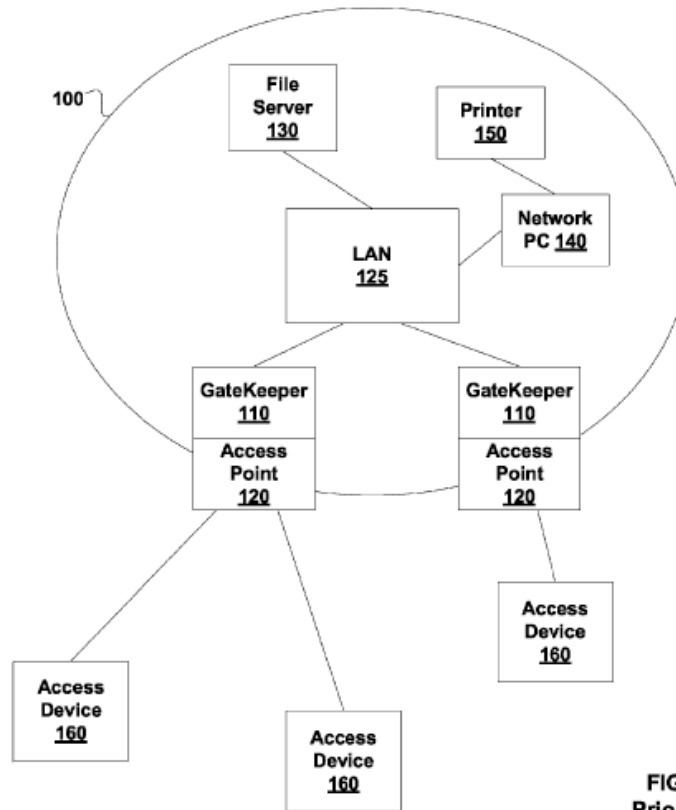


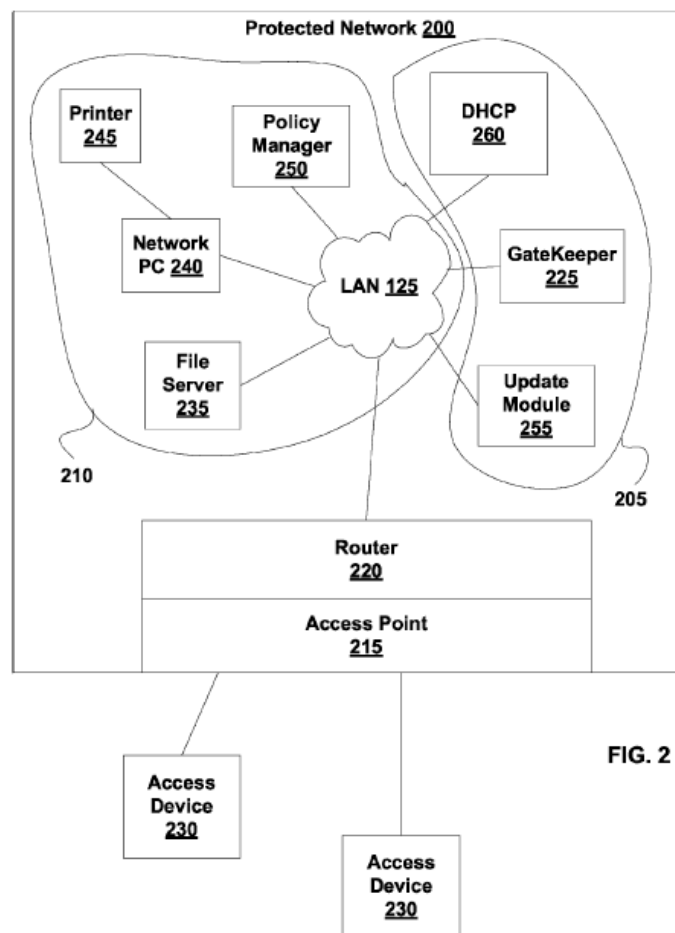
FIG. 1
Prior Art

Id. at Fig. 1. In Figure 1, access devices 160 communicate with access points 120, each of which connects with LAN 125 within secure network 100 through gatekeeper 110. *Id.* at 1:64–2:21. “A disadvantage of the use of GateKeeper 110, as practiced in the prior art, is that all communications between Access Device 160 and LAN 125 pass through GateKeeper 110,” which “can be a significant burden.” *Id.* at 2:34–39. The ’444 patent seeks to remove this disadvantage using “a protected network physically or logically divided into a restricted subset and one or more less-restricted subsets.” *Id.* at 2:56–58. “Requests from an access device for access to the less-restricted subset are first passed to the restricted subset,” and the gatekeeper is “then used to apply security policies to the

access device and if [the] security policies are satisfied, the access device is granted access to a less-restricted subset of the protected network.” *Id.*

at 2:58–64. “To grant access, the gatekeeper sends commands to the access point in order to reconfigure a communication port to which the access device is connected.” *Id.* at 3:28–30. “The reconfiguration typically includes reassigning the communication port from the restricted VLAN to the less-restricted VLAN.” *Id.* at 3:30–33.

Figure 2 of the ’444 patent depicts “a protected network, according to various embodiments of the invention.” Ex. 1201, 5:7–8. That figure is reproduced below.



Id. at Fig. 2. “Protected Network 200 is either physically or logically divided into a Restricted Subset 205 and a Less-Restricted Subset 210.” *Id.* at 5:59–61. Access devices 230 can connect to the protected network “through an Access Point 215 . . . and an optional Router 220.” *Id.* at 5:62–64. “[T]his access is under the control of a GateKeeper 225,” which is located within restricted subset 205 and which “is configured to enforce a security policy against” the access device. *Id.* at 5:64–67, Fig. 2.

The application that led to the ’444 patent was filed on June 14, 2012, and claims priority to, *inter alia*, a provisional application that was filed on September 24, 2003. Ex. 1001, codes (22), (60). Petitioner assumes a priority date of September 24, 2003, for purposes of this proceeding. Pet. 3. We discuss Patent Owner’s attempt to establish an earlier date of invention below. *See infra* § II.D.3.g.

D. Illustrative Claim

Of the challenged claims, claims 1 and 22 are independent. Claims 2–7, 10, 12, and 17 depend directly or indirectly from claim 1. Claim 1 is illustrative of the challenged claims and recites:

1. A method for auditing a device, the method comprising:
 - [1.1] performing an authentication using an EAP protocol from the device,
 - [1.2] the device being connected via a computer network to an access point configured to use an 802.1x protocol;
 - [1.3] sending a request for audit data to an agent running on the device;
 - [1.4] receiving the audit data at a gatekeeper configured to control access to a network, from the agent, the audit data pertaining to the device and having been obtained by the agent;
 - [1.5] applying a security policy that includes at least one requirements pertaining to the audit data and at least one requirement pertaining to the authentication, the applying of the security policy taking place under control of the gatekeeper.

Ex. 1201, 16:9–24 (Petitioner’s bracketed identifiers added); *see* Pet. vi (claim listing with Petitioner’s identifiers).²

E. Prior Art

Petitioner relies on the following prior art:

U.S. Patent Application Publication No. 2004/0111520 A1, filed Dec. 6, 2002, published June 10, 2004 (Ex. 1205, “Krantz”); and

U.S. Patent Application Publication No. 2004/0107360 A1, filed Mar. 13, 2003, published June 3, 2004 (Ex. 1206, “Herrmann”).

² Throughout this Decision, we reproduce the phrase “at least one requirements pertaining to the audit data” as it appears in limitation [1.5] despite the grammatical error.

F. The Asserted Ground

Petitioner challenges claims 1–7, 10, 12, 17, and 22 of the '444 patent based on the following ground (Pet. 3):

Claims Challenged	35 U.S.C. §	References
1–7, 10, 12, 17, 22	103(a) ³	Krantz, Herrmann

II. ANALYSIS

We now consider Petitioner’s asserted ground and Patent Owner’s arguments to determine whether Petitioner has met the “reasonable likelihood” standard for institution under 35 U.S.C. § 314(a).

A. Legal Standards

A claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the claimed subject matter and the 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. *See KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007).

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) where in evidence, so-called secondary

³ The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284, 287–88 (2011), amended 35 U.S.C. §§ 102 and 103. Because the '444 patent claims priority to an application filed before March 16, 2013 (the effective date of the relevant amendments), we assume that the pre-AIA versions of §§ 102 and 103 apply. However, our decision would be the same under the current version of the statutes.

considerations.⁴ *See Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). We also recognize that prior art references must be “considered together with the knowledge of one of ordinary skill in the pertinent art.” *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994) (citing *In re Samour*, 571 F.2d 559, 562 (CCPA 1978)).

B. Level of Ordinary Skill in the Art

Citing testimony from Dr. Houh, Petitioner contends that a person of ordinary skill in the art “would have had a bachelor’s degree in computer science, computer engineering, or an equivalent, and two years of relevant experience in networking and network security, and related fields.” Pet. 4. Petitioner also asserts that “[l]ack of professional experience can be remedied by additional education, and vice versa.” *Id.* Patent Owner argues that a person of ordinary skill in the art “would have had a bachelor’s degree in computer science, computer engineering, or electrical engineering and at least three years of experience in networking operating systems and cybersecurity.” Prelim. Resp. 1. Alternatively, Patent Owner argues that a person of ordinary skill in the art would have had “a master’s degree in one of the foregoing and at least two years of experience in the aforementioned fields.” *Id.* Patent Owner does not cite any evidence supporting its assessment of the level of ordinary skill. Neither party explains why the outcome of this case would be affected by the adoption of any of the proffered definitions of a person of ordinary skill in the art.

⁴ The present record does not include any evidence of secondary considerations of nonobviousness.

For purposes of this Decision, we adopt Petitioner’s definition of the level of ordinary skill in the art. On the present record, we are satisfied that this definition of the level of skill is consistent with the teachings of the ’444 patent and the asserted prior art.

C. Claim Interpretation

In an *inter partes* review, we construe each claim using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. [§] 282(b), including construing the 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). Accordingly, our claim construction standard is the same as that of a district court. *See id.* Under the standard applied by district courts, claim terms are generally given their plain and ordinary meaning, as would have been understood by a person of ordinary skill in the art at the time of the invention and in the context of the entire patent disclosure. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005) (en banc). “There are only two exceptions to this general rule: 1) when a patentee sets out a definition and acts as his own lexicographer, or 2) when the patentee disavows the full scope of a claim term either in the specification or during prosecution.” *Thorner v. Sony Comput. Entm’t Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012).

Petitioner argues that “a [person of ordinary skill in the art] would find the challenged claims unpatentable under any interpretation consistent with their plain and ordinary meaning in the context of the [’444 patent],” so we “need not expressly construe the claim terms.” Pet. 7. Patent Owner

argues “the claims should be given their plain meaning in the context of the intrinsic evidence.” Prelim. Resp. 6.

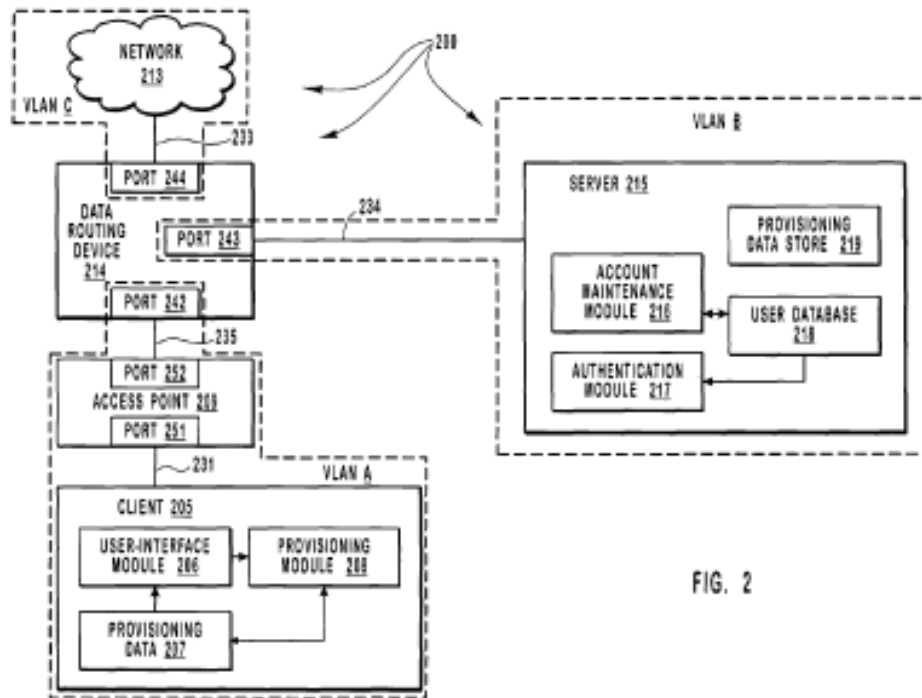
For purposes of this Decision, we determine that no aspects of the challenged claims require explicit construction. *See, e.g., Realtime Data, LLC v. Iancu*, 912 F.3d 1368, 1375 (Fed. Cir. 2019) (“The Board is required to construe ‘only those terms . . . that are in controversy, and only to the extent necessary to resolve the controversy.’” (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))).

D. Obviousness Ground Based on Krantz and Herrmann

Petitioner contends the subject matter of claims 1–7, 10, 12, 17, and 22 would have been obvious over the combination of Krantz and Herrmann. Pet. 20–88. Patent Owner disputes Petitioner’s contentions. Prelim. Resp. 11–42.

1. Krantz

Krantz is a U.S. patent application titled “Increasing the Level of Automation when Provisioning a Computer System to Access a Network.” Ex. 1205, code (54). Krantz “relates to configuring computer systems to appropriately communicate on a network, and more specifically, to automatically providing a computer system with appropriate information such that the computer system can be provisioned to communicate on a network.” *Id.* ¶ 2. Figure 2 of Krantz is reproduced below.



Id. at Fig. 2. Figure 2 “illustrates an example of a network architecture that can facilitate increasing the level of automation when provisioning a client.” *Id.* ¶ 28. In Figure 2, “[d]ata can be transferred between access po[in]t 209 and client 205 through port 251. Likewise, data can be transferred between access point 209 and data routing device 214 through port 252.” *Id.* ¶ 63. “Data routing device 214 can be configured to transfer both tagged data frames and untagged data frames between the VLANs depicted in FIG. 2.” *Id.* ¶ 60.

Petitioner contends that Krantz qualifies as prior art under 35 U.S.C. § 102(e) based on its filing date of December 6, 2002. Pet. 7; *see also* Ex. 1205, code (22). As discussed below, Patent Owner attempts to antedate Krantz. *See infra* § II.D.3.g.

2. *Herrmann*

Herrmann is a U.S. patent application titled “System and Methodology for Policy Enforcement.” Ex. 1206, code (54). Herrmann “relates generally to information processing and, more particularly, to systems and methods for policy enforcement on computer systems connected to one or more networks.” *Id.* ¶ 3. According to Herrmann, “if a client device connected to a network . . . is infected with a virus or worm, it may infect other machines on the same network,” making it important to “ensur[e] that devices connected to the network are running current anti-virus programs.” *Id.* ¶ 12. To do so, Herrmann teaches a system in which a client device attempts to access a network and information is collected “from the client device” so that the system can “determin[e] whether to authenticate the client device for access to the network based, at least in part, upon the collected information.” *Id.*, code (57).

Petitioner contends that Herrmann qualifies as prior art under 35 U.S.C. § 102(e) based on its filing date of March 13, 2003. Pet. 10; *see also* Ex. 1206, code (22). As discussed below, Patent Owner attempts to antedate Herrmann. *See infra* § II.D.3.g.

3. *Claim 1*

a. Preamble

The preamble of claim 1 recites “[a] method for auditing a device.” Ex. 1201, 16:9. Petitioner cites Krantz for teaching a server’s receipt of credentials (i.e., “audit data”) from client 205 (i.e., a “device”), whereupon the server may authorize at least partial access to a network. Pet. 20 (citing Ex. 1205 ¶¶ 16–17, 71, 74–76, 104, 107–109). According to Petitioner,

“[c]redentials supplied by the device/user in Krantz are used to control access to the protected network resources (‘*auditing a device*’).” *Id.* (citing Ex. 1203 ¶¶ 65–66; Ex. 1205 ¶¶ 16, 68–71, 99, 104, 107–109); *see also id.* at 21 (citing Ex. 1203 ¶ 68; Ex. 1205 ¶ 76) (similar argument). Petitioner also contends that “audit data” may include credentials such as user identifiers, passwords, and Extensible Authentication Protocol (EAP) Response/Identity messages from the client to the server.⁵ *Id.* at 20–21 (citing Ex. 1205 ¶¶ 18, 76).

Petitioner cites Dr. Houh’s testimony for the proposition that Krantz’s “access control process would be ‘*auditing*’ as the server of Krantz is inspecting credentials . . . and can authorize access based on the audit.” Pet. 20 (citing Ex. 1203 ¶¶ 65–66; Ex. 1205 ¶¶ 16, 71, 76, 104, 106–109). Petitioner further contends that, in accordance with the specification of the ’444 patent, user authentication can be part of an audit. *Id.* at 21 n.4 (citing Ex. 1201, 12:9–11).

Patent Owner does not dispute that Krantz teaches or suggests the preamble. Neither party addresses whether the preamble is limiting. “In general, a preamble limits the invention if it recites essential structure or steps, or if it is ‘necessary to give life, meaning, and vitality’ to the claim.” *Catalina Mktg. Int’l, Inc. v. Coolsavings.com, Inc.*, 289 F.3d 801, 808 (Fed. Cir. 2002) (citations omitted). “Conversely, a preamble is not limiting ‘where a patentee defines a structurally complete invention in the claim body

⁵ We note that Petitioner additionally maps “audit data” to Herrmann’s teachings of current security policy information/antivirus protection status in other parts of the Petition. *See, e.g.*, Pet. 35 (citing, *inter alia*, Ex. 1206 ¶¶ 64, 67), 43–44 (citing Ex. 1206 ¶¶ 12, 68), 51–52 (citing Ex. 1206 ¶¶ 12, 67–68).

and uses the preamble only to state a purpose or intended use for the invention.” *Id.* (citations omitted). At this juncture, we find that the preamble is not limiting because it only states the purpose/intended use of the method steps in the body of the claim. At trial, the parties should address whether the preamble is limiting, and, if so, whether Krantz’s access control process based on credentials (i.e., Krantz’s authentication process) (*see* Pet. 20–21) teaches “auditing” given Petitioner’s reliance on a similar analysis for teaching a separate limitation directed to “performing an authentication” (*see id.* at 24–28). We also note that Petitioner cites Herrmann’s teaching of checking for security policy information in conjunction with other limitations of claim 1. *See id.* at 35, 43–44, 51–52. To the extent the preamble is limiting, the parties should address whether Petitioner’s analysis from Herrmann for other limitations applies equally to the preamble for teaching “auditing.”

b. Limitations [1.1] and [1.2]

Claim 1 further recites “performing an authentication using an EAP protocol from the device, the device being connected via a computer network to an access point configured to use an 802.1x protocol.” Ex. 1201, 16:10–13. For “performing an authentication,” Petitioner cites Krantz’s teaching of a client sending credentials via an Extensible Authentication Protocol (EAP) Response/Identity message to a server. Pet. 24–25 (Ex. 1203 ¶¶ 73–74; Ex. 1205 ¶¶ 16, 18). Petitioner cites Krantz’s teaching of various EAP message exchange techniques, including “pass[ing] certificates, keys, and supported cipher suites” and “operating system credentials.” *See id.* at 26–27 (emphasis omitted). Petitioner contends that

an ordinarily skilled artisan would have understood these techniques to disclose “authenticating the device and/or user of client 205 (*performing an authentication using an EAP protocol from the device[]*)” before authorization is granted.” *Id.* at 27–28 (citing Ex. 1203 ¶ 78; Ex. 1217, 2).

For “the device being connected via a computer network to an access point,” Petitioner contends that Krantz’s client 205 (i.e., the “device”) is connected to access point 209 via network architecture. Pet. 28–30 (citing Ex. 1203 ¶¶ 82–84; Ex. 1205, ¶¶ 38, 63, Fig. 2). For the recitation directed to the access point using “an 802.1x protocol,” Petitioner cites Krantz’s teachings on access point 209 transferring data packets using EAP encapsulation over LANs (EAPOL), an 802.1x protocol. *Id.* at 30–31 (citing Ex. 1205 ¶¶ 69, 72).

At this juncture, Patent Owner does not dispute that Krantz teaches limitations [1.1] and [1.2]. Petitioner shows sufficiently that Krantz teaches performing an authentication of client 205 by sending credentials via an EAP message. *See, e.g.*, Ex. 1203 ¶ 78; Ex. 1205 ¶¶ 16, 18. Petitioner also shows sufficiently that Krantz’s client 205 is connected to access point 209 via a network (*see, e.g.*, Ex. 1203 ¶¶ 82–84; Ex. 1205, ¶¶ 38, 63, Fig. 2) and that access point 209 uses an 802.1x protocol (*see, e.g.*, Ex. 1205 ¶¶ 69, 72).

c. Limitation [1.3]

Claim 1 further recites “sending a request for audit data to an agent running on the device.” Ex. 1201, 16:14–15. Regarding “sending a request for audit data,” Petitioner cites Krantz’s teaching of client 205 and server 215 exchanging EAP messages with “certificates, keys, and supported cipher suites” or “other credential information” (i.e., “audit data”). Pet. 31

(citing Ex. 1205 ¶ 74); *see also id.* at 32 (citing Ex. 1205 ¶¶ 60, 63, 73–74) (similar analysis). Petitioner also notes that “a handshake protocol may be used between the access device and gatekeeper.” *Id.* at 31–32 (citing Ex. 1205 ¶¶ 13, 32, 72, 78, 99).

Petitioner acknowledges that “Krantz does not expressly state an agent is used,” but Petitioner contends it would have been obvious in view of Herrmann to use an agent such that “[t]he ‘*audit data*’ (EAP-messages, operating system credentials, certificates, keys, and supported cipher suites, etc.) disclosed in Krantz would be retrieved by, e.g., utilizing a client ‘*agent*.’” *Id.* at 33 (citing Ex. 1203 ¶ 89). Specifically, Petitioner cites Herrmann’s teaching of policy agent 413 “**retriev[ing] information about the current security policy in operation on the client device 310** [*i.e.*, ‘*request for audit data*’].” *Id.* at 34–35 (quoting Ex. 1206 ¶ 64) (citing Ex. 1206 ¶¶ 67, 80, 98, Fig. 4). In light of Krantz’s two stated goals involving automation and security, Petitioner contends an ordinarily skilled artisan would have been motivated “to add the security policy agent of Herrmann to the client device of Krantz” because Herrmann’s policy agent “would be complimentary to Krantz’s system in providing automated methods of network security.” *Id.* at 35–36 (citing Ex. 1203 ¶ 92; Ex. 1205 ¶¶ 14, 19). Petitioner notes that implementing Herrmann’s policy agent could be implemented with a simple software modification. *Id.* at 36 (citing Ex. 1203 ¶ 93).

Patent Owner does not dispute Petitioner’s analysis of limitation [1.3] at this juncture.⁶ Petitioner shows sufficiently that Herrmann teaches policy agent 413 on client device 310 for retrieving security policy information related to client device 310, which is a “request for audit data.” *See, e.g.*, Ex. 1206 ¶¶ 67, 80, 98, Fig. 4. In addition, we are persuaded preliminarily that an ordinarily skilled artisan would have had reason to implement Herrmann’s policy agent in Krantz’s client as a known automated means of providing network security. *See, e.g.*, Ex. 1203 ¶ 92; Ex. 1205 ¶¶ 14, 19.

d. Limitation [1.4]

Claim 1 further recites “receiving the audit data at a gatekeeper configured to control access to a network, from the agent, the audit data pertaining to the device and having been obtained by the agent.” Ex. 1201, 16:16–19. Petitioner relies on the combination of Krantz and Herrmann for teaching this limitation. *See* Pet. 36–37. Petitioner maps the recited “gatekeeper” to Krantz’s server 215 and contends that it “has the functionality to authorize access” based on credentials received from client 205 (i.e., the “device”). *Id.* at 38–39 (citing Ex. 1205 ¶¶ 16–17, 68–71, 74–76, 99, 104, 107–109). Petitioner cites step 307 in Krantz’s method 300 for provisioning a computer system (depicted in Figure 3), which pertains to “requesting authorization to access resources located on a second network.” *Id.* at 39–40 (emphasis omitted) (quoting Ex. 1205 ¶ 104) (citing Ex. 1205 ¶ 70, Fig. 3). Petitioner notes that step 307 may include the

⁶ Notwithstanding, Patent Owner disputes Petitioner’s rationale for combining Herrmann with Krantz. *See* Prelim. Resp. 18–21. We discuss Patent Owner’s arguments below. *See infra* § II.D.3.f.

“corresponding act of receiving user-entered information” from “a user at client 205,” i.e., step 303 of method 300. *Id.* at 40–41 (quoting Ex. 1205 ¶ 104).

To the extent that Krantz does not teach or suggest “receiving audit data,” Petitioner contends “[i]t would have been obvious to include Herrmann’s techniques for ‘receiving *audit data at a gatekeeper*’ (e.g., evaluating whether a device includes antivirus software) in the system of Krantz.” Pet. 42–43 (citing Ex. 1203 ¶¶ 105–106). According to Petitioner, “checking for anti-virus software would merely be an additional item for server 215 (*‘gatekeeper’*) to check in the authentication process disclosed by Krantz.” *Id.* at 43 (citing Ex. 1206 ¶¶ 12, 68). As motivation for the combination, Petitioner cites Krantz’s alleged focus on “network authentication/security.” *Id.* (citing Ex. 1205, code (57)).

Regarding the “gatekeeper configured to control access to a network,” Petitioner contends that Krantz’s VLAN B/network 412 and VLAN C/network 413 constitute a protected network. Pet. 44, 49. Petitioner cites Krantz’s teachings on controlling access to networks based on received credentials. *Id.* at 44–45 (citing Ex. 1205 ¶¶ 16–17). Petitioner also cites Krantz’s teachings of the server (within VLAN B) controlling access to a second network (within VLAN C). *See id.* at 47–50 (citing, *inter alia*, Ex. 1205 ¶¶ 16–17, 30, 52, 54, 71, 74–76, 104, 107–109, Figs. 2, 4).

For receiving “from the agent, the audit data pertaining to the device and having been obtained by the agent,” Petitioner acknowledges that Krantz does not disclose the gatekeeper receiving such audit data. Pet. 50. Thus, Petitioner relies on Herrmann’s teaching of policy agent 413 “retriev[ing] information about the current security policy in operation on the client

device 310” and policy server 460 “evaluat[ing] whether or not the client device 310 has a correct, up-to-date version of the applicable security policy.” *Id.* at 51 (emphasis omitted) (quoting Ex. 1206 ¶¶ 64, 67).

According to Petitioner, “the agent of Herrmann can obtain the ‘*audit data pertaining to the device*’ (e.g., antivirus software and applicable security policy status) and the gatekeeper can *receiv[e] the audit data ‘from the agent’* through a periodic check where the audit data is ‘*obtained by the agent*’ from the device.” *Id.* at 52 (citing Ex. 1203 ¶ 123); *see also id.* at 35 (citing Ex. 1206 ¶¶ 80, 98) (discussing Herrmann’s teaching of the policy server notifying the client (including policy agent 413) with periodic status messages). Petitioner likens Herrmann’s Network Access Server and Policy (Integrity) Server to the gatekeeper of Krantz and contends an ordinarily skilled artisan would have been motivated to add the security policy agent of Herrmann to the client device of Krantz because the “policy **agent** of Herrmann would be complimentary to the system of Krantz, as it would automate means of providing network security.” *Id.* at 52–54 (citing Ex. 1203 ¶¶ 123–124, 126; Ex. 1206 ¶¶ 53, 65, Fig. 4).

Patent Owner does not dispute Petitioner’s analysis of limitation [1.4] at this juncture. Based on the present record, Petitioner shows sufficiently that Krantz’s server 215 functions as a “gatekeeper” because it can control a client’s access to a network. *See, e.g.*, Ex. 1205 ¶¶ 16–17, 68–71, 74–76, 99, 104, 107–109, Fig. 3. Petitioner also establishes sufficiently that, in the combined Krantz–Herrmann system, the gatekeeper can receive “audit data” regarding antivirus software status (*see, e.g.*, Ex. 1206 ¶¶ 12, 68) from the client device. Petitioner also has shown sufficiently that Herrmann teaches

receiving this “audit data” from policy agent 413. *See, e.g., id.* ¶¶ 64, 67, 80, 98.

e. Limitation [1.5]

Claim 1 further recites “applying a security policy that includes at least one requirements pertaining to the audit data and at least one requirement pertaining to the authentication, the applying of the security policy taking place under control of the gatekeeper.” Ex. 1201, 16:20–24.

For “applying a security policy that includes at least one requirements pertaining to the audit data,” Petitioner cites Herrmann’s teaching of requiring updated antivirus software by “using security rules and checking system data [‘audit data’] for connecting devices to ascertain compliance.” Pet. 56–57 (emphasis omitted) (citing Ex. 1206 ¶¶ 12, 68, 71).

For the “at least one requirement pertaining to the authentication,” Petitioner cites Krantz’s teaching of authenticating users with credentials such as user identifier and password, operating system credentials, and EAP messages with certificates, keys, and supported cipher suites. Pet. 59–60 (citing Ex. 1205 ¶¶ 13, 32, 72, 74, 76, 78, 91, 99).

For “the applying of the security policy taking place under control of the gatekeeper,” Petitioner cites Krantz’s teaching of server 215 (i.e., the “gatekeeper”) authenticating a user when authentication module 217 favorably compares received credentials with entries in user database 218. Pet. 55 (citing Ex. 1205 ¶ 76). Petitioner contends the gatekeeper of Krantz can enforce security policies pertaining to “audit data” via EAP messages with certificates, keys, and supported cipher suites. *Id.* at 55–56 (citing Ex. 1205 ¶ 74). Petitioner also contends it would have been obvious to

apply Herrmann’s teachings on checking antivirus software status to the gatekeeper of Krantz. *Id.* at 57; *see also* Ex. 1203 ¶ 135 (similar testimony from Dr. Houh). Petitioner notes the similarity between Herrmann’s network access server (NAS) 320 and server 215 (i.e., the “gatekeeper”) of Krantz. Pet. 57 (citing Ex. 1206 ¶¶ 53, 65).

Patent Owner disputes that the Krantz–Herrmann combination teaches the “applying a security policy” limitation of claim 1. Prelim. Resp. 12–17. Patent Owner argues that “Krantz teaches authentication, but not ‘audit data’” and that Petitioner “improperly conflate[s] ‘audit data’ and ‘authentication’ to mean the same thing.” *Id.* at 12; *see also id.* at 15–16 (similar argument that “Krantz only discloses user authentication”). In contrast, Patent Owner argues that the ’444 patent “explains that ‘audit data pertaining to a device’ is data about the device’s software and/or hardware necessary to comply with the security policy.” *Id.* at 13–14 (citing Ex. 1201, 11:48–59). Petitioner also argues that authentication is different from “audit data pertaining to a device” particularly given that “the claims [of the ’444 patent] recite authentication and auditing separately” and given that Figure 4 of the ’444 patent shows authentication and obtaining audit data as “distinct elements.” *Id.* at 14–15 (citing Ex. 1201, Fig. 4, claim 1).

Patent Owner also argues that “[t]he Petition relies on Herrmann only for an agent on a device,” and thus Herrmann “is not relevant to the ‘applying a security policy’ limitation.” Prelim. Resp. 17 (citing Pet. 50). Patent Owner criticizes Petitioner’s analysis because Petitioner allegedly asserts that “Herrmann’s supposed ‘audit data’ would be evaluated through Krantz[’s] ‘authentication process’” rather than “the audit process which is a separate claim element.” *Id.*

We do not agree with Patent Owner’s arguments because Patent Owner overlooks Petitioner’s reliance on Herrmann for teaching “audit data.” In particular, Petitioner expressly relies on “Herrmann’s techniques for obtaining system data from an access device (e.g., whether it includes antivirus software) in the system of Krantz.” Pet. 14. Although we agree with Patent Owner that Petitioner frequently cites Krantz’s credential information as “audit data,” Petitioner also cites Herrmann’s teaching of “information about the current security policy in operation on the client device 310.” Pet. 35 (emphasis omitted) (citing, *inter alia*, Ex. 1206 ¶¶ 64, 67); *see also id.* at 43–44 (citing Ex. 1206 ¶¶ 12, 68) (similar analysis related to the proof of specific virus-protection programs as “audit data”), 51–52 (citing Ex. 1206 ¶¶ 12, 67–68) (same).

We are persuaded preliminarily that Krantz’s authentication module, as modified by Herrmann’s disclosures on checking for approved antivirus programs, teaches the “applying a security policy” limitation with a requirement pertaining to “audit data.” *See, e.g.*, Ex. 1203 ¶¶ 133–134; Ex. 1206 ¶¶ 12, 68, 71. Krantz’s authentication module also checks for credentials, which sufficiently teaches a requirement pertaining to “authentication.” *See, e.g.*, Ex. 1205 ¶¶ 13, 32, 72, 74, 76, 78, 91, 99. We also are persuaded preliminarily that it would have been obvious to apply Herrmann’s teachings on checking antivirus status to Krantz’s server 215 (i.e., the “gatekeeper”), which determines whether to allow access to a network. *See, e.g.*, Ex. 1203 ¶ 135; Ex. 1205 ¶¶ 74, 76.

f. Rationale for Combining Krantz and Herrmann

Petitioner contends that “[i]t would have been obvious to include Herrmann’s techniques for obtaining system data from an access device (e.g., whether it includes antivirus software) in the system of Krantz.”

Pet. 14. Petitioner notes that Krantz teaches authentication module 217 in server 215 checking user credentials as part of an authentication and authorization process for client 205. *Id.* (citing Ex. 1205 ¶¶ 72, 76).

Petitioner also notes Herrmann’s teaching of policy server 460 enforcing security policies and rules, such as a policy requiring a specific virus protection program to be operational on a client. *Id.* at 14–15 (citing Ex. 1206 ¶¶ 12, 68). As such, Petitioner contends that an ordinarily skilled artisan “would [have] recognize[d] that checking for anti-virus software would simply be an additional item for authentication module 217 (of server 215) to check in the authentication process already disclosed in Krantz.” *Id.* at 14; *see also* Ex. 1203 ¶ 52 (similar testimony from Dr. Houh).

Petitioner proposes modifying Krantz’s authentication module, which checks user credentials against a database, so that it also would check for approved antivirus programs according to Herrmann’s teachings. Pet. 15. Petitioner contends that “[i]nformation regarding approved antivirus software and connected devices could be stored in the User Database or an additional Database could be added.” *Id.* (citing Ex. 1203 ¶ 53). Petitioner argues that an ordinarily skilled artisan “would have had a reasonable expectation of success in implementing these techniques into a combined Krantz/Herrmann system as it would involve minimal changes to the existing Krantz system.” *Id.* at 19 (citing Ex. 1203 ¶ 64).

Petitioner further contends that an ordinarily skilled artisan “would have been motivated to apply Herrmann’s technique of checking connecting computer systems for antivirus software as it would provide added security and increase automation when connecting to a network.” *Id.* at 19 (citing Ex. 1206 ¶ 68). According to Petitioner, “[s]ecurity and automation are two stated goals of Krantz.” *Id.* (citing Ex. 1205 ¶¶ 14, 19). Therefore, Petitioner contends that an ordinarily skilled artisan “would have recognized that Herrmann’s policy server disclosure checking for compliance with an antivirus security policy, would be complimentary to Krantz, which seeks an automated process for providing network security.” *Id.*; *see also* Ex. 1203 ¶ 64 (similar testimony from Dr. Houh).

Patent Owner disputes that an ordinarily skilled artisan would have been motivated to combine Herrmann with Krantz. Prelim. Resp. 18–21. Patent Owner cites the statement in the ’444 patent specification that “[t]he method used to support auditing functionality over the existing 802.1x protocol implementation is complicated and not an obvious variation of the 802.1x protocol.” *Id.* at 18 (quoting Ex. 1201, 14:11–13). It is not clear, however, how the alleged complexity of the disclosed process undermines Petitioner’s particular rationale for the combination. And, aside from the arguments discussed above regarding “applying a security policy,” Patent Owner does not argue that Petitioner’s proposed combination fails to teach the recited process steps of claim 1.

Patent Owner also criticizes Petitioner’s assertion that Krantz’s focus on “authentication and security” would have provided motivation for the combination. *See* Prelim. Resp. 19–21. Patent Owner argues that Krantz is limited to authentication and includes nothing about auditing. *Id.* at 19

(citing Ex. 1205, code (57); Ex. 2001 ¶¶ 49, 57–59). Given the alleged absence of any teaching on security policy compliance in Krantz, Patent Owner characterizes Petitioner’s stated rationale as being based on impermissible hindsight. *Id.* at 19–20 (citing *Polaris Indus., Inc. v. Arctic Cat, Inc.*, 882 F.3d 1056, 1068 (Fed. Cir. 2018)). Further, to the extent Krantz mentions “security,” Patent Owner argues that this only relates to user authentication. *Id.* at 20–21 (citing Ex. 1205 ¶ 16; Ex. 2001 ¶¶ 49, 57–59).

Based on the present record, we find Petitioner’s rationale sufficient for institution. Petitioner points to Krantz’s alleged goals of security and automation. Pet. 19. Petitioner (*id.*) and Dr. Houh (Ex. 1203 ¶ 64) both cite paragraph 19 of Krantz, which states that “[i]f credentials do not authorize full access . . . the server can respond by sending a notification . . . includ[ing] conditions (e.g., signup, renewal etc.) a user must satisfy to become authorized for []full access to resources.” Ex. 1205 ¶ 19. We are persuaded preliminarily that an ordinarily skilled artisan considering Krantz’s teachings of such conditions for full access would have had reason to apply Herrmann’s technique for checking a client’s antivirus security policy in the manner suggested by Petitioner. *See, e.g.*, Ex. 1203 ¶ 64; Ex. 1206 ¶ 68. Krantz’s express teaching of conditions for a client to fully access a network (Ex. 1205 ¶ 19) also undermines Patent Owner’s argument about impermissible hindsight and Patent Owner’s suggestion that Krantz is limited to user authentication. Finally, we are persuaded that an ordinarily skilled artisan would have expected success in making the combination because it would only require software modifications to Krantz’s system. *See, e.g.*, Ex. 1203 ¶¶ 65, 93.

g. Patent Owner's Argument Regarding the Prior-Art Status of Krantz and Herrmann

Patent Owner argues that neither Krantz nor Herrmann qualifies as prior art under pre-AIA 35 U.S.C. § 102(e) “because the InfoExpress inventors conceived of the invention before the effective dates and exercised reasonably continuous diligence in reducing to the claimed inventions to practice.” Prelim. Resp. 30. In particular, Patent Owner asserts a conception date of no later than November 14, 2002, which is the date of a document titled “CyberGatekeeper LAN Based Policy Enforcement Engineering Specification.” *Id.* at 32 (citing Ex. 2011). Patent Owner further contends that “InfoExpress exercised reasonably continuous diligence up and through at least the filing of” the provisional patent application to which the ’444 patent claims priority. *Id.* at 33; *see also id.* at 33–41 (alleging details and citing evidence regarding diligence). Patent Owner contends that the filing of the provisional patent application evidences constructive reduction to practice. *Id.* at 33, 42.

Petitioner disagrees that the present record sufficiently shows that the inventors of the ’460 patent conceived of the invention before the effective date of Krantz or Herrmann and that the inventors exercised reasonably continuous diligence in reducing that invention to practice. Prelim. Reply 1–7. In particular, Petitioner raises questions with respect to the independence of Patent Owner’s evidence from the inventor testimony that evidence is intended to corroborate, as well as with respect to whether the evidence offered by Patent Owner sufficiently shows conception, reduction to practice, and reasonably continuous diligence. *Id.*

We do not think the present record shows that Patent Owner has antedated both Krantz and Herrmann sufficiently to warrant denying

institution of *inter partes* review on that basis. First, Patent Owner's arguments rely on the testimony of inventor Stacey C. Lum, who has not yet been subject to cross-examination. Prelim. Resp. 32–41 (citing Ex. 2003). Second, Petitioner identifies several issues where further development of the record may be helpful. For example, Patent Owner's asserted date of conception is associated with the date of the document titled "CyberGatekeeper LAN Based Policy Enforcement Engineering Specification." See Prelim. Resp. 32 (citing Ex. 2003 ¶ 12; Ex. 2011; Ex. 2012). We agree with Petitioner (*see* Prelim. Reply 4–5) that it is unclear, based on the present record, whether this document corroborates the testimony supporting Patent Owner's conception date given that the present record does not establish the author of the document. See Ex. 2003 ¶ 22 (inventor Stacey C. Lum testifying only that "InfoExpress personnel drafted EX2011, entitled 'LAN Based Policy Enforcement Engineering Specification'"). These and other issues relating to the prior-art status of Krantz and Herrmann are, in our view, best left for trial after full development of the record.

h. Conclusion Regarding Claim 1

Petitioner has shown sufficiently at this juncture that the combination of Krantz and Herrmann teaches all limitations of claim 1. Petitioner also has put forth a sufficient rationale for combining Herrmann with Krantz with a reasonable expectation of success. Based on the present record, we determine that Petitioner has established a reasonable likelihood that it would prevail in showing that the subject matter of claim 1 would have been obvious over the combination of Krantz and Herrmann.

4. *Claims 2–7 and 22*

We have already determined that Petitioner has established a reasonable likelihood of success that it would prevail in showing that claim 1 would have been obvious over the combination of Krantz and Herrmann, and we will be instituting review on all challenged claims for the asserted ground. *See SAS Inst. Inc. v. Iancu*, 138 S. Ct. 1348 (2018) (holding that the Board may not institute review on fewer than all claims challenged in the petition); 37 C.F.R. § 42.108(a) (“When instituting *inter partes* review, the Board will authorize the review to proceed on all of the challenged claims and on all grounds of unpatentability asserted for each claim.”). Nevertheless, we include the following discussion regarding claims 2–7 and 22.

Claims 2–7 and 22 all require that “applying the security policy includes configuring the access point.” *See, e.g.*, Ex. 1201, 16:25–26 (claim 2). Petitioner argues, *inter alia*, that Krantz’s disclosure of the configuration of access point 209 “as a VLAN aware device [that] can insert Tag Headers into data frames received from client 205 . . . that are to be transferred to VLAN B and/or VLAN C” teaches “configuring the access point.” Pet. 62 (quoting Ex. 1205 ¶ 64). In particular, Petitioner argues that when Krantz’s access point inserts Tag Headers that enable access to VLAN C, access point 209/communication port 251 is configured. *Id.* at 63 (citing Ex. 1203 ¶ 144). This is because, according to Petitioner, port 251 inserts Tag Headers within access point 209. *Id.* at 63–64 (citing, *inter alia*, Ex. 1203 ¶¶ 144–145; Ex. 1205 ¶ 107).

Patent Owner argues that “Krantz discloses no configuring of access point 209 at all” and instead configures “[d]ata frames in client data,” which

Patent Owner likens to “[a]dding a header to an envelope.” Prelim. Resp. 25–26.

On the present record, we find Petitioner’s contentions regarding “configuring the access point” sufficient for institution. Petitioner shows sufficiently, based on the present record, that Krantz teaches or suggests such configuring when access point 251 inserts Tag Headers that enable access to VLAN C. Ex. 1205 ¶ 64. Further, Dr. Houh testifies that the insertion of Tag Headers is accomplished by port 251 within access point 209. Ex. 1203 ¶ 145 (citing Ex. 1207, 11; Ex. 1208, 4:42–47; Ex. 1209, 16:4–13; Ex. 1210, 210). Dr. Houh’s testimony is not conclusory and is supported by citation to additional information that would have been known to a person of ordinary skill in the art. *Id.* On the present record, this testimony appears not to be contradicted by other evidence.

Patent Owner additionally argues that claims 5–7 “include limitations related to updated audit data.” Prelim. Resp. 28. Patent Owner criticizes Petitioner’s analysis to the extent it relies on Krantz’s teachings on authentication. *Id.* Yet Petitioner also relies on Herrmann’s teachings of the client notifying the policy server once necessary steps have been taken to comply with an assigned policy. *See, e.g.,* Pet. 78 (citing Ex. 1206 ¶ 80). We find this teaching from Herrmann sufficient to teach “updated audit data.”

5. *Remaining Challenged Claims*

Patent Owner either relies on the same arguments discussed above or does not present separate arguments for the remaining challenged claims. Given that we will be instituting *inter partes* review on all claims, it is not

necessary for us to provide an assessment of Petitioner's challenges regarding the remaining challenged claims. Those challenges, in our view, are best left for trial after full development of the record.

III. CONCLUSION

After considering the evidence and arguments presented in the current record, we determine that Petitioner has demonstrated a reasonable likelihood that it would prevail with respect to at least one of the claims challenged in the Petition. Accordingly, we institute an *inter partes* review on all of the challenged claims and the ground presented in the Petition. At this stage of the proceeding, we have not made a final determination as to the patentability of the challenged claims.

IV. ORDER

Accordingly, it is

ORDERED that pursuant to 35 U.S.C. § 314, *inter partes* review is instituted as to claims 1–7, 10, 12, 17, and 22 of the '444 patent with respect to the ground of unpatentability presented in the Petition; and

FURTHER ORDERED that *inter partes* review is commenced on the entry date of this Order, and pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, notice is hereby given of the institution of a trial.

IPR2024-00677
Patent 8,578,444 B2

PETITIONER:

Scott Border
Winston & Strawn LLC
sborder@winston.com

Patrick McPherson
Patrick Muldoon
David Dotson
DUANE MORRIS LLP
pdmcperson@duanemorris.com
pcmuldoon@duanemorris.com
dcdotson@duanemorris.com

PATENT OWNER:

Brian R. Michalek
Joseph M. Kuo
Brian R. Landry
Saul Ewing LLP
Brian.Michalek@saul.com
Joseph.Kuo@saul.com
Brian.Landry@saul.com