

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.,
Petitioner,

v.

LIONRA TECHNOLOGIES LTD.,
Patent Owner.

IPR2023-00669
Patent 7,302,708 B2

Before PATRICK R. SCANLON, JO-ANNE M. KOKOSKI, and
STEVEN M. AMUNDSON, *Administrative Patent Judges*.

AMUNDSON, *Administrative Patent Judge*.

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

I. INTRODUCTION

Cisco Systems, Inc. (“Petitioner”) filed a Petition requesting an *inter partes* review of claims 1–6 and 9 in U.S. Patent No. 7,302,708 B2 (Exhibit 1001, “the ’708 patent”) under 35 U.S.C. §§ 311–319. Paper 2 (“Pet.”). Along with the Petition, Petitioner filed a Notice of Filing of Two *Inter Partes* Review Petitions. Paper 3 (“Notice”). Lionra Technologies Ltd. (“Patent Owner”) filed a Preliminary Response. Paper 7 (“Prelim. Resp.”). No further briefing was requested or authorized.

Under 37 C.F.R. § 42.4(a), we have authority to determine whether to institute an *inter partes* review. We may institute an *inter partes* review only if “the information presented in the petition filed under section 311 and any response filed under section 313 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.” 35 U.S.C. § 314(a) (2018). The “reasonable likelihood” standard is “a higher standard than mere notice pleading” but “lower than the ‘preponderance’ standard to prevail in a final written decision.” *Hulu, LLC v. Sound View Innovations, LLC*, IPR2018-01039, Paper 29 at 13 (PTAB Dec. 20, 2019) (precedential).

Based on the current record and for the reasons explained below, Petitioner has shown that there is a reasonable likelihood that it would prevail with respect to at least one of the challenged claims. Thus, we institute an *inter partes* review of claims 1–6 and 9 in the ’708 patent on all challenges included in the Petition.

II. BACKGROUND

A. Real Parties in Interest

Petitioner identifies itself as the real party in interest. Pet. 79. Patent Owner identifies itself as the real party in interest. Paper 4, 2. The parties do not raise any issue about real parties in interest.

B. Related Matters

Petitioner and Patent Owner identify the following civil actions as related matters involving the '708 patent:

- *Lionra Technologies Ltd. v. Cisco Systems, Inc.*, No. 2:22-cv-00305 (E.D. Tex. filed Aug. 8, 2022);
- *Lionra Technologies Ltd. v. Fortinet, Inc.*, No. 2:22-cv-00322 (E.D. Tex. filed Aug. 19, 2022) (the “lead Texas case”); and
- *Lionra Technologies Ltd. v. VMware, Inc.*, No. 1:23-cv-00929 (W.D. Tex. filed Aug. 7, 2023).

Pet. 79; Paper 4, 2; Prelim. Resp. 3; Paper 8, 2. Patent Owner explains that the above-identified civil actions in the Eastern District of Texas were consolidated with the following civil action in the Eastern District of Texas: *Lionra Technologies Ltd. v. Palo Alto Networks, Inc.*, No. 2:22-cv-000334 (E.D. Tex. filed Aug. 29, 2022). Prelim. Resp. 3; *see* Ex. 2001 (Order Consolidating Cases).

In related IPR2023-00670, Petitioner challenges claims 10–14 in the '708 patent. Notice 2; *see* Paper 4, 2; Paper 8, 2.

C. The '708 Patent (Exhibit 1001)

The '708 patent, titled “Enforcing Computer Security Utilizing an Adaptive Lattice Mechanism,” issued on November 27, 2007, from an application filed on March 11, 2004. Ex. 1001, codes (22), (45), (54). The

patent states that the “inventive arrangements relate generally to computer and information security and more particularly to security measures that enforce security based on logical implementation methods.” *Id.* at 1:8–11; *see id.* at code (57).

The ’708 patent describes controlling access to information and computer resources as a “continuing problem for system, database, and network administrators across the government, military, and private industry.” Ex. 1001, 1:13–16. According to the patent, “[p]roviding system security in such multiuser environments requires a balance between permitting access to resources necessary to perform the business functions for the enterprise and limiting access.” *Id.* at 1:16–19.

The ’708 patent explains that conventional security methods “fall within two basic categories”: physical implementation methods and logical implementation methods. Ex. 1001, 1:19–21. The patent notes that the prior art discloses the following security features:

- “accessing portions of information based on user access authority”;
- “utiliz[ing] an inheritance graph to propagate changes in security descriptors”; and
- “utiliz[ing] a neural network and a set of rules to track usage patterns and flag suspicious activities.”

Id. at 1:33–51 (citing Ex. 1007 (U.S. Patent No. 6,453,418 B1); Ex. 1008 (U.S. Patent No. 6,446,077 B2); Ex. 1010 (U.S. Patent No. 6,334,121 B1)).

The ’708 patent also explains that conventional security methods for “implementing logical security safeguards typically provide access based on a user/group/role identifier and an access control list for the file, database, or system function to be accessed.” Ex. 1001, 1:22–25. According to the

patent, however, “there are a number of serious limitations to such an approach, primarily because control over information access is limited to a simple relational comparison.” *Id.* at 1:25–28. Additionally, conventional security systems do not (1) “enforce security based on patterns of behavior, aggregation of data, or information clustering” or (2) “support the ability to look at” temporal access patterns. *Id.* at 1:28–32.

The ’708 patent discloses systems and methods for “ensuring secure access to a computer system” that determine if an “access request completes a prohibited temporal access pattern.” Ex. 1001, 1:55–64, code (57); *see id.* at 2:62–63, 9:55–65. “If so, the request is rejected.” *Id.* at 1:64.

The ’708 patent also discloses “logically organizing the computer system in the form of a tree hierarchy having a plurality of leaf nodes and higher-level nodes.” Ex. 1001, 2:7–9; *see id.* at 2:65–3:2. “A plurality of the base nodes can be defined as comprising respectively a plurality of leaf nodes of the tree hierarchy.” *Id.* at 2:9–11; *see id.* at 3:45–48. Higher-level nodes represent aggregations of the base nodes and/or temporal access patterns. *Id.* at 2:11–12, 3:2–3. Each node in the tree hierarchy “can have an associated security level representing the mandatory security level for the particular aggregation or pattern.” *Id.* at 3:4–6.

The '708 patent's Figure 1 (reproduced below) depicts a computer system organized in the form of a tree hierarchy:

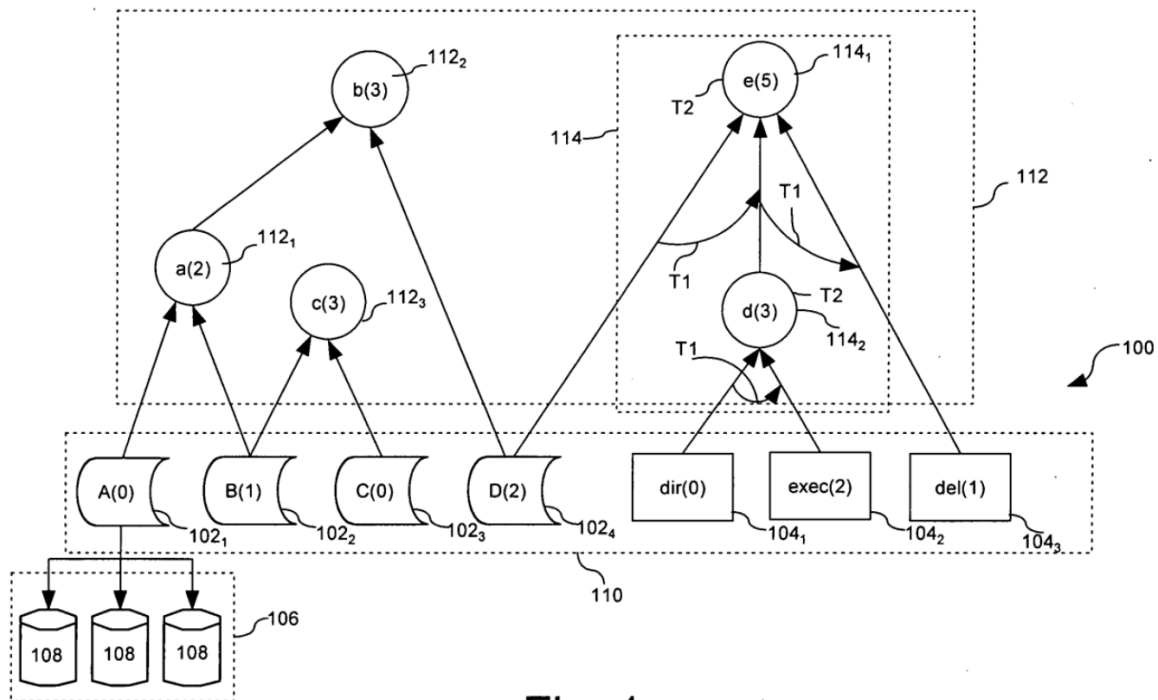


Fig. 1

Figure 1 illustrates hierarchical tree 100 including “a plurality of leaf or base nodes 110” and higher-level nodes 112 “constructed to represent aggregations of base nodes 110 . . . as well as higher order aggregations, i.e. aggregations of previously constructed aggregations.” Ex. 1001, 3:43–52, Fig. 1; *see id.* at 2:37–38, 6:13–16.

As Figure 1 shows, base nodes 110 include a plurality of object types 102₁, 102₂, 102₃, and 102₄ and a plurality of system functions 104₁, 104₂, and 104₃. Ex. 1001, 3:10–12, Fig. 1. Object types 102₁, 102₂, 102₃, and 102₄ represent information types A, B, C, and D, respectively. *Id.* at 3:12–13, Fig. 1. “Instantiations 106 of object types can include multiple type instances 108.” *Id.* at 3:13–14, Fig. 1. System functions 104₁, 104₂,

and 104₃ represent functions that a process or user can access, i.e., “directory (dir), execute (exec), and delete (del)” in Figure 1. *Id.* at 3:27–31, Fig. 1.

Each object type and system function “can have a minimum required security access level associated therewith.” Ex. 1001, 3:15–16, 3:34–39. The ’708 patent sometimes calls the object types and system functions “security access primitives.” *See id.* at 2:37–38, 2:64–3:2.

In Figure 1, “a number in parenthesis” specifies the minimum required security access level for a process or user to access the associated object type or system function. Ex. 1001, 3:15–19, 3:34–39, Fig. 1. As an example, object type 102₄ includes the label “D(2)” where the number “2” in parenthesis indicates that “information type D has a minimum required security access level of two.” *Id.* at 3:19–22. As another example, system function 104₂ includes the label “exec(2)” where the number “2” in parenthesis indicates that “a process or user [must] possess a security level of at least two in order to access that function.” *Id.* at 3:39–42.

As Figure 1 shows, “relationships can be asserted for temporal access patterns.” Ex. 1001, 4:4–5, Fig. 1. Specifically, “the curved arrows labeled T1 denote a temporal ordering between the accesses defined by items 114₁ and 114₂.” *Id.* at 4:4–6, Fig. 1.

As an example, item 114₂ in Figure 1 denotes a temporal ordering between items 104₁ and 104₂ as follows: “104₁→104₂” such that item 104₁ precedes item 104₂ in that temporal ordering. Ex. 1001, 4:6–8, Fig. 1. Hence, node d(3) in Figure 1 “not only identifies an aggregation of the primitive functions denoted by 104₁ and 104₂ but also specifies that an explicit temporal ordering exists in that 104₁ is accessed before 104₂.” *Id.* at 4:8–11. Further, “for the security policy associated with item 114₂ to be

activated, not only must both 104₁ and 104₂ be accessed but they must be accessed in the order indicated by the temporal relationship.” *Id.* at 4:11–16. Thus, if item 104₂ is “accessed first followed by item 104₁, the security policy associated with” node d(3) “will not be activated because the temporal order was not satisfied.” *Id.* at 5:45–48.

As another example, item 114₁ in Figure 1 denotes a temporal ordering between items 102₄, 114₂, and 104₃ as follows: “102₄→114₂→104₃” such that item 102₄ precedes item 114₂ and item 114₂ precedes item 104₃ in that temporal ordering. Ex. 1001, 4:17–22, Fig. 1. Because item 114₂ is “an aggregation of access operations,” the “operations identified by item 114₂ become subsumed into the overall temporal ordering of item 114₁ and the full temporal order is 102₄→104₁→104₂→104₃, where item 114₂ in the original temporal order has been replaced by its constituent parts, 104₁→104₂.” *Id.* at 4:22–29.

The ’708 patent’s Figure 4B (reproduced below) depicts a temporal access table:

Temporal Access Table (TAT)

Usr	A	B	C	D	dir	exec	del
1(1)					102	112	
2(1)							
3(2)					111	103	
4(1)							
5(3)							

Fig. 4B

Figure 4B illustrates a temporal access table with the following rows and columns:

- five rows corresponding to the five users identified as 1(1), 2(1), 3(2), 4(1), and 5(3), where the number in parentheses denotes the user's security access level;
- four columns corresponding to the four information types A, B, C, and D; and
- three columns corresponding to the three system functions directory (dir), execute (exec), and delete (del).

Ex. 1001, 5:55–56, Fig. 4B. The temporal access table “maintains a history of the primitive operations performed by a user.” *Id.* at 5:55–57. “As a user is granted authorization to perform a primitive access operation, the operation is timestamped and stored” in the temporal access table. *Id.* at 5:57–59; *see id.* at 7:7–12, 7:65–8:5.

As Figure 4B shows, “user 1 performed a dir operation at time 102 and then requested an exec operation at time 112.” Ex. 1001, 5:61–63, Fig. 4B. Because the dir operation (item 104₁ in Figure 1) precedes the exec operation (item 104₂ in Figure 1), the security policy associated with node d(3) identifies a prohibited temporal access pattern and denies the request. *Id.* at 5:63–66; *see id.* at code (57). In contrast to user 1, user 3 performed an exec operation at time 103 and then requested a dir operation at time 111. *Id.* at 5:66–6:1, Fig. 4B. Because that sequence does not match a prohibited temporal access pattern, “the operations are permitted.” *Id.* at 6:1–2.

The '708 patent explains that higher-level nodes 112 “will often have a higher minimum required security level” relative to base nodes 110 “because aggregated data is often of a more sensitive nature.” Ex. 1001, 6:16–23. “Consequently aggregated information will inevitably be of

greater interest to unauthorized users.” *Id.* at 6:23–25. Thus, “system administrators will naturally wish to impose higher level restrictions on its access.” *Id.* at 6:25–26.

The ’708 patent also explains that “access to all of the information types or system functions associated with base nodes 110 that are participants in a particular aggregation node is, in many instances, tantamount to directly accessing the aggregation node.” Ex. 1001, 6:27–32. Hence, “it can be desirable to increase the required security authorization level for a particular user to access a base node to be at least equal to the security authorization level of an aggregation node to which the base node is a participant.” *Id.* at 6:38–42; *see id.* at 2:16–33, 6:32–38. For instance, after “identifying within the hierarchy any nodes that directly or indirectly comprise children of any of the higher-level nodes that are aggregations” comprising a first base node, the “minimum required entity access level” can be “updated for any base nodes that directly or indirectly comprise children of any of the higher-level nodes that are aggregations comprising the first base node.” *Id.* at 2:16–23; *see id.* at 7:25–39, 8:10–42, 9:5–23.

D. The Challenged Claims

Petitioner challenges the following claims:

- independent claim 1 for a method for secure access to a computer system;
- claims 2–6 that depend directly or indirectly from claim 1; and
- independent claim 9 for a method for restricting access to a computer system.

Pet. 1, 24, 26–75.

Claims 1 and 9 exemplify the challenged claims and read as follows (with formatting added for clarity and with bracketed numbers and letters added for reference purposes):¹

1. [1pre] A method for secure access to a computer system, comprising the steps of:

[1a] receiving in said computer system a request from an entity with a predetermined access level for access to a first base node representing at least one of an information type and a computer system function;

[1b] determining if said access request completes a prohibited temporal access pattern for said entity;

[1c] comparing a minimum access level established for said first base node to said predetermined access level;

[1d] granting said access request only if it does not complete a prohibited temporal access pattern for said entity, and said minimum access level for said first base node does not exceed said predetermined access level; and

[1e] denying said request if said access request completes a prohibited temporal access pattern for said entity.

9. [9pre] A method for restricting access to a computer system having a plurality of logical base nodes representing at least one of an information type and a computer system function, and a plurality of higher-level nodes arranged together with said base nodes in the form of a tree hierarchy, comprising the steps of:

[9a] receiving in said computer system a request from an entity with a predetermined access level for access to a first base node;

[9b] determining if said access request completes a prohibited temporal access pattern for said entity;

¹ We use the same numbers and letters that Petitioner uses to identify the claim language. *See* Pet. 10, 37–58, 67–69.

[9c] comparing a minimum access level established for said first base node to said predetermined access level;

[9d] granting said access request only if it does not complete a prohibited temporal access pattern for said entity, and said minimum access level for said first base node does not exceed said predetermined access level; and

[9e] denying said request if said access request completes a prohibited temporal access pattern for said entity.

Ex. 1001, 10:16–31, 11:15–33.

E. The Asserted References

For its challenges, Petitioner relies on the following references:

Name	Reference	Exhibit
Gladstone	US 7,290,266 B2, issued October 30, 2007 (based on an application filed February 8, 2002)	1004
Hada	US 2005/0076030 A1, published April 7, 2005 (based on an application filed August 29, 2003)	1005
Salazar	US 2004/0122792 A1, published June 24, 2004 (based on an application filed December 20, 2002)	1009

Pet. 24, 26–75. Petitioner asserts that each reference qualifies as prior art under § 102(e). *Id.* at 24–25; *see* 35 U.S.C. § 102(e) (2006).²

At this stage of the proceeding, Patent Owner does not dispute that each reference qualifies as prior art. *See* Prelim. Resp. 1–17.

² The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284 (2011), amended 35 U.S.C. § 102 and § 103 effective March 16, 2013. Because the filing date of the challenged claims predates the AIA’s amendments to § 102 and § 103, this decision refers to the pre-AIA versions of § 102 and § 103.

F. The Asserted Challenges to Patentability

Petitioner asserts the following challenges to patentability:

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1–5, 9	103(a)	Gladstone, Salazar
6	103(a)	Gladstone, Salazar, Hada

Pet. 24, 26–75.

G. Testimonial Evidence

To support its challenges, Petitioner relies on the declaration of Paul C. Clark, Ph.D. (Exhibit 1003). Dr. Clark states, “I received a Bachelor of Science in Mathematics from the University of California Irvine, a Master of Science in Electrical Engineering and Computer Science from the University of Southern California, and a Doctor of Science in Electrical Engineering and Computer Science from The George Washington University.” Ex. 1003 ¶ 11. Dr. Clark also states, “I have been retained by Cisco Systems, Inc. (Petitioner) as an independent, technical expert consultant in this proceeding” and “have been asked to provide my technical expertise, analysis, insights and opinions regarding” the ’708 patent and relevant references. *Id.* ¶¶ 2, 9.

At this stage of the proceeding, Patent Owner does not introduce testimonial evidence concerning the patentability issues.

III. DISCRETIONARY DENIAL UNDER § 314(a)

Under § 314(a), the Director possesses “broad discretion” in deciding whether to institute an *inter partes* review. *See* 35 U.S.C. § 314(a); *Saint Regis Mohawk Tribe v. Mylan Pharm. Inc.*, 896 F.3d 1322, 1327 (Fed. Cir. 2018). The Director is “permitted, but never compelled,” to institute an *inter partes* review. *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1367

(Fed. Cir. 2016). The Board decides whether to institute an *inter partes* review on the Director's behalf. 37 C.F.R. § 42.4(a) (2023).

A. Discretionary Denial in View of Parallel Litigation

Patent Owner argues that we should exercise our discretion under § 314(a) to deny institution in view of the lead Texas case. *See* Prelim. Resp. 1–11; *supra* § II.B. Petitioner argues that we should decline to exercise our discretion under § 314(a) to deny institution. *See* Pet. 76–79. For the reasons explained below, we decline to exercise our discretion under § 314(a) to deny institution in view of the lead Texas case.

1. NONEXCLUSIVE FACTORS TO CONSIDER

When deciding whether to exercise discretion under § 314(a) to deny institution, the Board has considered the status of litigation involving the parties in light of the AIA's objective "to provide an effective and efficient alternative to district court litigation." *NHK Spring Co. v. Intri-Plex Techs., Inc.*, IPR2018-00752, Paper 8 at 12, 19–20 (PTAB Sept. 12, 2018) (precedential). The Board has set forth the following nonexclusive factors to consider when determining whether to exercise discretion under § 314(a) to deny institution due to the advanced state of parallel litigation:

- (1) whether the court granted a stay or evidence exists that one may be granted if the Board institutes a trial;
- (2) the proximity of the court's trial date to the Board's projected statutory deadline for a final written decision;
- (3) the investment in the parallel litigation by the court and the parties;
- (4) the overlap in the issues raised by the petition and the issues in the parallel litigation;
- (5) whether the petitioner and the defendant in the parallel litigation are the same party; and

- (6) other circumstances that impact the Board’s exercise of discretion, including the merits.

Apple Inc. v. Fintiv, Inc., IPR2020-00019, Paper 11 at 5–6 (PTAB Mar. 20, 2020) (precedential) (“*Fintiv*”).

These factors “relate to whether efficiency, fairness, and the merits support the exercise of authority to deny institution in view of an earlier trial date in the parallel proceeding.” *Fintiv*, IPR2020-00019, Paper 11 at 6. Further, *Fintiv* instructs that the Board should take “a holistic view of whether efficiency and integrity of the system are best served by denying or instituting review.” *Id.*; see PTAB Consolidated Trial Practice Guide at 55–56, 58 (Nov. 2019) (“CTPG”).³

We also follow the Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation (June 21, 2022) (“Interim Procedure”).⁴

2. ANALYSIS

The Interim Procedure explains that “the PTAB will not discretionarily deny institution in view of parallel district court litigation where a petitioner presents a stipulation not to pursue in a parallel proceeding the same grounds or any grounds that could have reasonably been raised before the PTAB.” Interim Procedure at 3 (citing *Sotera Wireless, Inc. v. Masimo Corp.*, IPR2020-01019, Paper 12 (PTAB Dec. 1, 2020) (precedential as to § II.A)); see *id.* at 7, 9. The Interim Procedure also

³ Available at <https://www.uspto.gov/TrialPracticeGuideConsolidated>.

⁴ Available at https://www.uspto.gov/sites/default/files/documents/interim_proc_discretionary_denials_aia_parallel_district_court_litigation_memo_20220621_.pdf.

explains that such a stipulation (a *Sotera* stipulation) “mitigates concerns of potentially conflicting decisions and duplicative efforts between the district court and the PTAB.” *Id.* at 7.

Petitioner provides a *Sotera* stipulation. Paper 9, Attach. A.
Specifically, Petitioner stipulates as follows:

if the PTAB institutes IPR on claims on the ground presented in the petition, Petitioners [sic] will not pursue against such claims in the co-pending district court litigation the specific ground asserted in the petition, or any other ground that was raised or could have been reasonably raised in an IPR (i.e., grounds that could have been raised under §§ 102 or 103 on the basis of prior art patent [sic] or printed publications).

Id. (emphasis omitted) (citing *Sotera*, IPR2020-01019, Paper 12 at 18–19).

Because Petitioner provides a *Sotera* stipulation, we decline to exercise our discretion under § 314(a) to deny institution in view of the lead Texas case. *See* Interim Procedure at 3, 7, 9.

B. Discretionary Denial Due to Multiple Petitions

1. BACKGROUND

In this proceeding, Petitioner challenges claims 1–6 and 9 in the ’708 patent. Pet. 24, 26–75; Prelim. Resp. 13. In particular, Petitioner contends that claims 1–5 and 9 are unpatentable under § 103(a) as obvious over Gladstone and Salazar and that claim 6 is unpatentable under § 103(a) as obvious over Gladstone, Salazar, and Hada. Pet. 24, 26–75.

In IPR2023-00670, Petitioner challenges claims 10–14 in the ’708 patent. Notice 2; Prelim. Resp. 13. In particular, Petitioner contends that claims 10–14 are unpatentable under § 103(a) as obvious over Gladstone and Salazar. IPR2023-00670, Paper 2 (Pet.) at 38–86.

Petitioner initiated this proceeding and IPR2023-00670 on the same day by filing parallel petitions. *See, e.g.*, Prelim. Resp. 1, 9, 13–14.

2. THE *GENERAL PLASTIC* FACTORS

In *General Plastic*, the Board discussed the “potential for abuse” due to multiple, staggered petitions “challenging the same patent and same claims.” *Gen. Plastic Indus. Co. v. Canon Kabushiki Kaisha*, IPR2016-01357, Paper 19 at 17 (PTAB Sept. 6, 2017) (precedential as to § II.B.4.i) (“*General Plastic*”). The Board said, “The absence of any restrictions on follow-on petitions would allow petitioners the opportunity to strategically stage their prior art and arguments in multiple petitions, using our decisions as a roadmap, until a ground is found that results in the grant of review.” *Id.*

In *General Plastic*, the Board identified the following nonexclusive factors to consider when deciding whether to exercise discretion under § 314(a) to deny institution based on a follow-on petition:

- (1) whether the same petitioner previously filed a petition directed to the same claims of the same patent;
- (2) whether at the time of filing of the first petition the petitioner knew of the prior art asserted in the second petition or should have known of it;
- (3) whether at the time of filing of the second petition the petitioner already received the patent owner’s preliminary response to the first petition or received the Board’s decision on whether to institute review in the first petition;
- (4) the length of time that elapsed between the time the petitioner learned of the prior art asserted in the second petition and the filing of the second petition;
- (5) whether the petitioner provides adequate explanation for the time elapsed between the filings of multiple petitions directed to the same claims of the same patent;

- (6) the finite resources of the Board; and
- (7) the requirement under 35 U.S.C. § 316(a)(11) to issue a final determination not later than 1 year after the date on which the Director notices institution of review.

Gen. Plastic, IPR2016-01357, Paper 19 at 9–10, 16.

Roadmapping concerns are “minimized,” however, when (1) “a petitioner files a later petition that raises unpatentability challenges substantially overlapping with those” in an earlier petition and (2) “the later petition is not refined based on lessons learned from later developments.”

Code200, UAB v. Bright Data Ltd., IPR2022-00861, Paper 18 at 5 (PTAB Aug. 23, 2022) (precedential); *see Expedia, Inc. v. Express Mobile, Inc.*, IPR2022-00785, Paper 16 at 9 (PTAB Sept. 27, 2022).

3. PATENT OWNER’S POSITION

Based on the *General Plastic* factors, Patent Owner urges the Board to exercise discretion under § 314(a) to deny institution in both this proceeding and IPR2023-00670. *See* Prelim. Resp. 1, 12–17; IPR2023-00670, Paper 7 (Prelim. Resp.) at 1, 12–17. Specifically, Patent Owner asserts that *General Plastic* factors (1), (2), and (6) favor discretionary denial and that factors (3), (4), (5), and (7) are neutral. Prelim. Resp. 13–17.

Regarding factor (1), Patent Owner argues that the challenged claims in this proceeding and the challenged claims in IPR2023-00670 are “closely related because they are directed to the same inventive concepts.” Prelim. Resp. 13. Further, Patent Owner asserts that “[i]f the claims were not closely related, then petitioner would not have been able to rely on the same combination of the same two references” and make “essentially the same conclusory arguments against all but one of the claims.” *Id.* at 13–14.

Regarding factor (2), Patent Owner argues that Petitioner “relies upon the same combination of the same two references – Gladstone and Salazar – in both” proceedings. Prelim. Resp. 14. According to Patent Owner, “Petitioner plainly knew of the prior art asserted in the first petition when it filed the second petition.” *Id.*

Regarding factor (6), Patent Owner argues that it and the Board will face “substantial and unnecessary burdens” if the Board institutes review in both this proceeding and IPR2023-00670. Prelim. Resp. 16. But Patent Owner admits that the “petitions are remarkably similar, as demonstrated by Petitioner’s reliance on the same two references – Goldstone [sic] and Salazar – in all of its invalidity challenges.” *Id.* at 15.

4. *GENERAL PLASTIC* DOES NOT APPLY HERE

General Plastic does not apply here because Petitioner did not file multiple, staggered petitions “challenging the same patent and same claims” and different petitioners did not challenge the same patent at different times. *See Gen. Plastic*, IPR2016-01357, Paper 19 at 9–10, 16–17; *see also Valve Corp. v. Elec. Scripting Prods., Inc.*, IPR2019-00062, Paper 11 at 9 (PTAB Apr. 2, 2019) (precedential). Instead, Petitioner initiated this proceeding and IPR2023-00670 on the same day by filing parallel petitions. *See, e.g.*, Prelim. Resp. 1, 9, 13–14. Thus, these circumstances do not implicate the roadmapping concerns that *General Plastic* seeks to alleviate. *See Gen. Plastic*, IPR2016-01357, Paper 19 at 16–17.

5. ANALYSIS OF PARALLEL PETITIONS

Patent Owner acknowledges that the PTAB Consolidated Trial Practice Guide discusses parallel petitions. *See* Prelim. Resp. 14–15 (quoting CTPG at 59). That Guide includes the following guidance:

Parallel Petitions Challenging the Same Patent. Based on the Board’s experience, one petition should be sufficient to challenge the claims of a patent in most situations. Two or more petitions filed against the same patent at or about the same time (e.g., before the first preliminary response by the patent owner) may place a substantial and unnecessary burden on the Board and the patent owner and could raise fairness, timing, and efficiency concerns. *See* 35 U.S.C. § 316(b). In addition, multiple petitions by a petitioner are not necessary in the vast majority of cases. To date, a substantial majority of patents have been challenged with a single petition.

Nonetheless, the Board recognizes that there may be circumstances in which more than one petition may be necessary, including, for example, when the patent owner has asserted a large number of claims in litigation or when there is a dispute about priority date requiring arguments under multiple prior art references. . . .

CTPG at 59; *see* Prelim. Resp. 14–15 (quoting CTPG at 59).

Patent Owner argues that “[t]his is not a situation where more than one petition is necessary” because Patent Owner has asserted only five claims (claims 1, 2, 9, 10, and 11) in the parallel litigation, not “a large number of claims.” Prelim. Resp. 15; *see* Ex. 2007, 2.

But Petitioner does not contend that Patent Owner has asserted “a large number of claims” in the parallel litigation. *See* Notice 2–5. Rather, Petitioner provides the following reasons for filing two petitions:

- (1) claims 1–6 and 9 at issue in this proceeding are method claims;
- (2) claims 10–14 at issue in IPR2023-00670 are system claims;
- (3) claims 10, 11, 13, and 14 recite “processing means” that “could invoke the means-plus-function provisions of pre-AIA 35 U.S.C. § 112, sixth paragraph”;

- (4) claims 10, 11, 13, and 14 include “lengthy associated functions”;
- (5) the “Board’s rules require Petitioner to construe any potentially means-plus-function terms, including identifying the corresponding structure disclosed in the specification”;
- (6) Petitioner “devote[d] a substantial portion” of the 14,000 word-count limit to the potential constructions of claims 10, 11, 13, and 14 under § 112, sixth paragraph, in the petition in IPR2023-00670; and
- (7) Petitioner “found it infeasible to comply with the claim construction rule, the word count rule, and its obligation to explain the grounds of unpatentability” in a single petition.

Id. at 2–4 (citing *Williamson v. Citrix Online, LLC*, 792 F.3d 1339, 1350 (Fed. Cir. 2015); 37 C.F.R. §§ 42.24(a)(1)(i), 42.104(b)(3)–(b)(5)).

Petitioner explains that it challenges claims 10–14 in “a second petition so that the Board may be presented with the complete claim analysis for all challenged claims.” *Id.* at 4.

Additionally, Petitioner explains that if the Board determines that “the ‘processing means’ terms of claims 10, 11, 13 and 14 invoke § 112, sixth paragraph,” the Board could also determine that “the specification provides insufficient disclosure for the Board to construe claims 10–14 and evaluate claims 1–6 and 9 relative to the prior art.” Notice 4. Petitioner asserts that “[i]t would be unfair and counterproductive for the Board to be prevented from evaluating the unpatentability of the non-means-plus-function claims over the prior art simply because of the means-plus-function claims’ potential invalidity under § 112.” *Id.* Petitioner also asserts that the “presentation of separate petitions” challenging claims 1–6 and 9 in this

proceeding and claims 10–14 in IPR2023-00670 “facilitates the Board’s consideration of each challenge.” *Id.* at 5.

Patent Owner does not address Petitioner’s reasons for filing two petitions. *See, e.g.*, Prelim. Resp. 12–17.

We agree with Petitioner that the circumstances here justify two petitions. *See* Notice 2–5. As Petitioner asserts, Petitioner “devote[d] a substantial portion” of the 14,000 word-count limit to the potential constructions of claims 10, 11, 13, and 14 under § 112, sixth paragraph, in the petition in IPR2023-00670. *See id.* at 3; IPR2023-00670, Paper 2 (Pet.) at 13–28. As Petitioner also asserts, the “presentation of separate petitions” challenging claims 1–6 and 9 in this proceeding and claims 10–14 in IPR2023-00670 “facilitates the Board’s consideration of each challenge.” *See* Notice 5.

Under the circumstances here, conducting two related *inter partes* reviews will not stress the Board’s finite resources or unduly burden the Board or Patent Owner. In this proceeding and IPR2023-00670, the prior art and the unpatentability arguments largely overlap. Specifically, Petitioner cites Gladstone and Salazar when arguing the obviousness of each challenged claim in each proceeding and additionally cites Hada in this proceeding when arguing the obviousness of claim 6. Pet. 26–75; Prelim. Resp. 13–15; IPR2023-00670, Paper 2 (Pet.) at 39–86. Also, as Patent Owner admits, the challenges in each proceeding involve similar unpatentability arguments based on Gladstone and Salazar, e.g., “essentially the same” arguments in “remarkably similar” petitions according to Patent Owner. *See* Pet. 36–69; Prelim. Resp. 13–15; IPR2023-00670, Paper 2 (Pet.) at 49–86.

6. CONCLUSION CONCERNING DISCRETIONARY DENIAL DUE TO MULTIPLE PETITIONS

For the reasons discussed above, we decline to exercise our discretion under § 314(a) to deny institution due to multiple petitions.

IV. PATENTABILITY ANALYSIS

A. Legal Principles: Obviousness

A patent may not be obtained “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 at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.” 35 U.S.C. § 103(a) (2006). An obviousness analysis involves underlying factual inquiries including (1) the scope and content of the prior art; (2) differences between the claimed invention and the prior art; (3) the level of ordinary skill in the art; and (4) where in evidence, objective indicia of nonobviousness, such as commercial success, long-felt but unsolved needs, and failure of others.⁵ *Graham v. John Deere Co.*, 383 U.S. 1, 17–18, 35–36 (1966); *Apple Inc. v. Samsung Elecs. Co.*, 839 F.3d 1034, 1047–48 (Fed. Cir. 2016) (en banc). When evaluating a combination of references, an obviousness analysis should address “whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007).

We analyze the obviousness issues according to these principles.

⁵ The record does not include evidence or argument regarding objective indicia of nonobviousness.

B. Level of Ordinary Skill in the Art

Factors pertinent to determining the level of ordinary skill in the art include (1) the educational level of the inventor; (2) the type of problems encountered in the art; (3) prior-art solutions to those problems; (4) the rapidity with which innovations are made; (5) the sophistication of the technology; and (6) the educational level of workers active in the field. *Envtl. Designs, Ltd. v. Union Oil Co.*, 713 F.2d 693, 696–97 (Fed. Cir. 1983). Not all factors may exist in every case, and one or more of these or other factors may predominate in a particular case. *Id.* These factors are not exhaustive, but merely a guide to determining the level of ordinary skill in the art. *Daiichi Sankyo Co. v. Apotex, Inc.*, 501 F.3d 1254, 1256 (Fed. Cir. 2007). Moreover, the prior art itself may reflect an appropriate skill level. *Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001).

Petitioner asserts that a person of ordinary skill in the art at the time of the alleged invention “would have had at least a Bachelor’s degree in Computer Science, Computer Engineering, or a similar degree and at least two years of professional experience with computer systems, including computer-security and access-control methods.” Pet. 13. Petitioner also asserts that “[m]ore experience can supplement less education and vice versa.” *Id.* Dr. Clark’s testimony supports Petitioner’s assertions. *See* Ex. 1003 ¶¶ 56–57.

At this stage of the proceeding, Patent Owner does not address the level of ordinary skill in the art. *See* Prelim. Resp. 1–17.

Based on the current record and for purposes of this decision, we accept Petitioner’s description of an ordinarily skilled artisan because it

comports with the technology and claims of the '708 patent as well as the asserted prior art.

C. Claim Construction

We construe claim terms “using the same claim construction standard” that district courts use to construe claim terms in civil actions under 35 U.S.C. § 282(b). *See* 37 C.F.R. § 42.100(b). Under that standard, claim terms “are given their ordinary and customary meaning, which is the meaning the term would have to a person of ordinary skill in the art at the time of the invention.” *Power Integrations, Inc. v. Fairchild Semiconductor Int’l, Inc.*, 904 F.3d 965, 971 (Fed. Cir. 2018) (citing *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005) (en banc)). The meaning of claim terms may be determined by “look[ing] 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).

Petitioner contends that each term in each challenged claim in this proceeding should have “its plain and ordinary meaning.” Pet. 12–13 (citing Ex. 1003 ¶ 41). Petitioner also contends that “no specific construction of any claim term is required because the prior art relied on in this Petition meets each of the claim terms under any reasonable construction.” *Id.* at 13 (citing Ex. 1003 ¶ 41).

At this stage of the proceeding, Patent Owner does not address claim construction. *See* Prelim. Resp. 1–17.

“[O]nly those terms need be construed that are in controversy, and only to the extent necessary to resolve the controversy.” *Vivid Techs., Inc. v.*

Am. Sci. & Eng'g, Inc., 200 F.3d 795, 803 (Fed. Cir. 1999); *see Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017). Based on the current record, we determine that no claim term requires an explicit construction to decide whether Petitioner satisfies the “reasonable likelihood” standard for instituting trial.

D. Alleged Obviousness over Gladstone and Salazar: Claims 1–5 and 9

Petitioner contends that claims 1–5 and 9 are unpatentable under § 103(a) as obvious over Gladstone and Salazar. *See* Pet. 26–69. Below, we provide overviews of Gladstone and Salazar, and then consider the obviousness issues. As explained below, Petitioner establishes sufficiently for purposes of institution that the combined disclosures in Gladstone and Salazar teach the subject matter in claims 1–5 and 9.

1. OVERVIEW OF GLADSTONE (EXHIBIT 1004)

Gladstone is a U.S. patent titled “Access Control by a Real-Time Stateful Reference Monitor with a State Collection Training Mode and a Lockdown Mode for Detecting Predetermined Patterns of Events Indicative of Requests for Operating System Resources Resulting in a Decision to Allow or Block Activity Identified in a Sequence of Events Based on a Rule Set Defining a Processing Policy,” filed on February 8, 2002, and issued on October 30, 2007. Ex. 1004, codes (12), (22), (45), (54). Gladstone states that the invention concerns “software that controls an operating policy of a computer system,” e.g., to allow or block “access to various system resources, such as files and network connections.” *Id.* at 1:22–25; *see id.* at code (57).

Gladstone describes a “reference monitor” as “a component of a computer system that determines whether an access by one component,

for example a user process, of another component, for example, a file is permitted.” Ex. 1004, 1:64–67. According to Gladstone, conventional operating systems include stateless reference monitors that “determine whether a particular access to a file or other resource is permitted.” *Id.* at 2:7–12. In “most cases the access decision is made based on the identity of the user whose local program or process makes the request and one or more static permissions flags or an access control list associated with the resource.” *Id.* at 2:16–20.

Some conventional operating systems “give finer control by associating individual permissions with each user.” Ex. 1004, 2:30–31. Other conventional operating systems “are even finer grained, and allow individual users to offer a set of tokens, and if any match those found in the access controllist, then access is granted.” *Id.* at 2:36–39.

Gladstone identifies deficiencies in conventional operating systems. Ex. 1004, 3:17–42. Among other things, conventional systems “do not detect or control access based on [a] pattern of behavior.” *Id.* at 3:17–19. Hence, “conventional systems cannot detect and react to attacks in which diverse parts of the attack are performed by seemingly normal operations of diverse programs or processes, that only form the attack when taken in combination.” *Id.* at 3:38–42.

To address that deficiency in conventional operating systems, Gladstone discloses a stateful reference monitor that controls access to a file or other resource based on a “pattern of activity” or “sequence of actions.” *See* Ex. 1004, 1:46–55, 5:17–24, 6:44–54, 7:25–35, 9:11–22, 9:43–55, 10:1–39, 11:63–65, 12:22–26, 13:8–10, 16:28–31, 16:39–40, 17:21–22, code (57), Figs. 1–2. For instance, the stateful reference monitor may use

a “sequence of actions” to detect “normal behavior” as well as “malicious behavior.” *Id.* at 13:8–17; *see id.* at 9:55–58.

The stateful reference monitor “retains and relies on changing system state information in implementing decision policies.” Ex. 1004, 5:32–36; *see id.* at 9:43–46. The stateful reference monitor “maintains an updateable storage area whose contents can be used to affect access decisions.” *Id.* at code (57).

The stateful reference monitor “acts as an additional processing step over and above any existing stateless reference monitor in the operating system.” Ex. 1004, 10:48–50. Thus, the stateful reference monitor “cannot grant access when the standard stateless reference monitor would have denied access.” *Id.* at 10:50–52.

Gladstone's Figure 1 (reproduced below) depicts a software system with a stateful reference monitor:

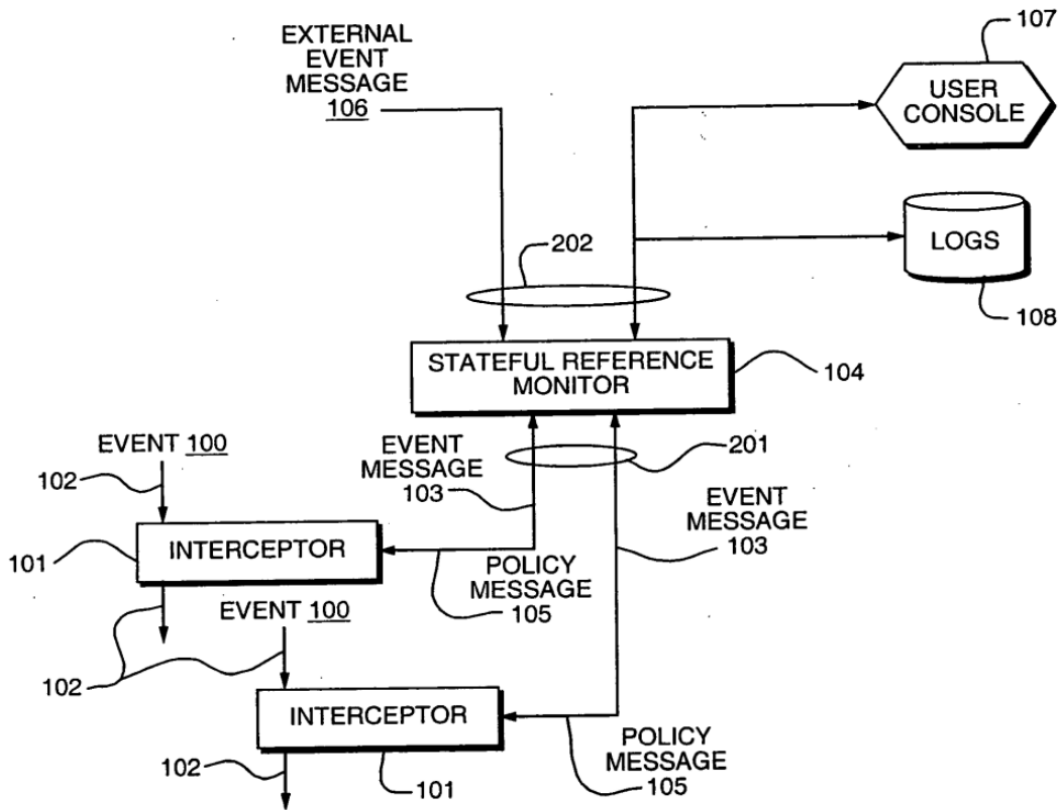


FIG. 1

Figure 1 illustrates a software system including interceptors 101, stateful reference monitor 104, user console 107, and log files 108. Ex. 1004, 4:53–54, 5:16–28, Fig. 1. The software system (1) monitors “events 100, e.g. access requests to a resource,” and (2) controls “the effect of those events, e.g. blocking or allowing the requested access to a resource.” *Id.* at 5:6–9; *see id.* at 6:38–42.

Interceptors 101 “interact with the operating system” by intercepting “various types of operating system requests,” called “events,” including “requests for access to operating system resources such as a file or network connection.” Ex. 1004, 6:38–42; *see id.* at 9:62–64. In particular,

“interceptors 101 are inserted in the control or communication paths 102 traversed by those events.” *Id.* at 5:10–12; *see id.* at 6:62–64.

During normal operations, interceptor 101 intercepts event 100, generates event message 103, and then sends event message 103 to stateful reference monitor 104 for a stateful access decision. Ex. 1004, 5:16–18, 6:42–44, 7:25–35, Fig. 1. After receiving event message 103 from interceptor 101, stateful reference monitor 104 “returns a policy message 105 to the interceptor 101.” *Id.* at 5:18–19; *see id.* at 6:48–51, 12:1–4. “The policy message 105 may be an action for the interceptor 101 to take, such as allowing an access request event 100 to continue along the control or communication path 102 to have its intended effect, or not allowing the event 100 to pass along path 102.” *Id.* at 5:19–24; *see id.* at 6:52–54.

Gladstone’s Figure 2 (reproduced below) depicts Figure 1’s software system in more detail:

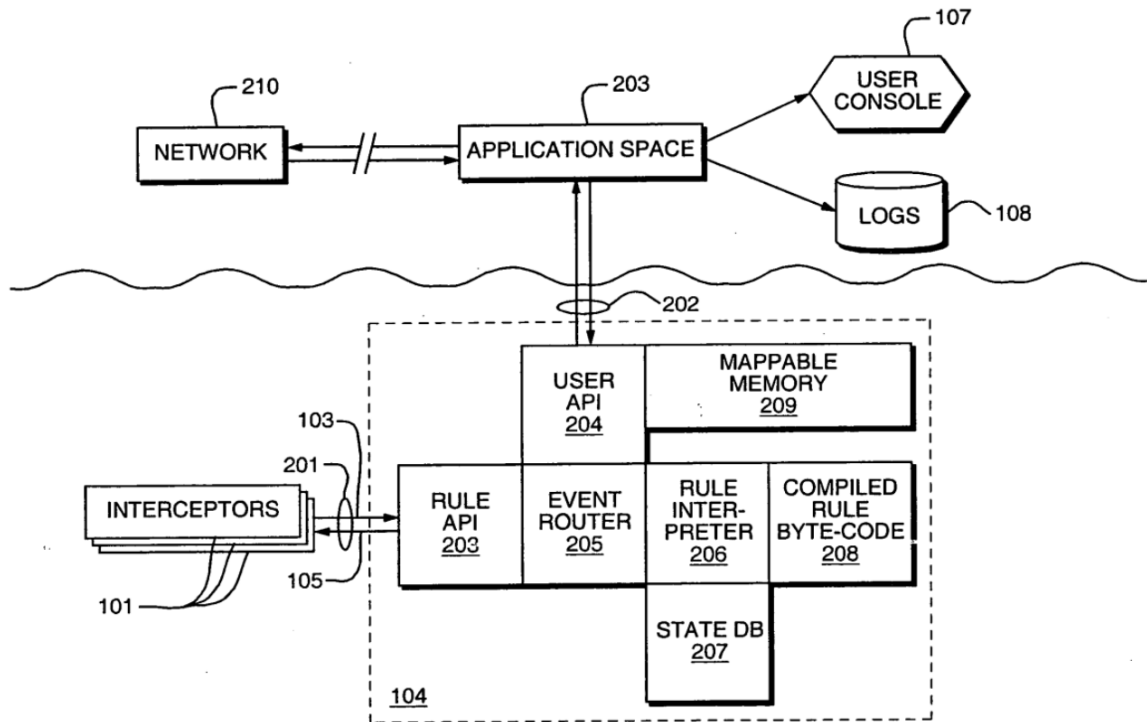


FIG. 2

Figure 2 illustrates a software system including interceptors 101, stateful reference monitor 104, various components in stateful reference monitor 104, user console 107, log files 108, and application space 203. Ex. 1004, 4:55–56, 5:16–28, 5:37–44, Fig. 2.

As Figure 2 shows, stateful reference monitor 104 “communicates with other parts of the operating system and with applications through” communication channels 201 and 202. Ex. 1004, 5:37–39, Fig. 2. Communication channel 201 “carries event messages 103 and policy messages 105.” *Id.* at 5:39–40. Communication channel 202 “carries external event messages 106, as well as other messages to and from

application space 203, including but not limited to messages to and from the user console 107 and logs 108.” *Id.* at 5:41–44.

As Figure 2 also shows, stateful reference monitor 104 includes the following components:

- (1) rule API 203 for interfacing with communication channel 201;⁶
- (2) user API 204 for interfacing with communication channel 202;
- (3) event router 205 for “directing and controlling all internal communication”;
- (4) rule interpreter 206 for processing event messages and selecting rules;
- (5) state database 207 for storing dynamic state information and event information, such as the “time of the event, type of event, application generating the event, user owning the application and the like”;
- (6) compiled rule byte-code 208 for storing rules that implement “the operational policies to be enforced and against which activities and state in the system are checked”; and
- (7) mappable memory 209 for providing a “memory addressable by both the stateful reference monitor 104 and other applications, such that data transfer may be easily accomplished by writing to and reading from a predetermined location, without requiring special communication apparatus, mechanisms or protocols.”

Ex. 1004, 5:45–57, 5:63–64, 6:1–3, 6:9–11, 6:24–34, 6:44–51, 7:35–48, 8:4–18, 8:57–60, 9:11–13, 9:36–39, 9:59–61, 10:66–11:16, Fig. 2.

⁶ Gladstone uses the acronym “API” to mean “application programming interface.” *See* Ex. 1004, 5:47.

Gladstone explains that state information includes “information that a certain event occurred within a certain time of the present time.” Ex. 1004, 6:13–15. Gladstone also explains that stateful reference monitor 104 “ensures that requests are ordered, i.e. a request either happens before or after another request.” *Id.* at 12:22–24.

Gladstone discloses an example of a “prohibited combination” of events X, Y, and Z (combination X-Y-Z) where stateful reference monitor 104 prohibits event Z if events X and Y have already occurred, i.e., “a rule in byte-code 208 will prohibit Z.” Ex. 1004, 6:15–19. Additionally, “another rule in byte-code 208 will cause event X and/or event Y to be purged from state database 207 after a suitable time.” *Id.* at 6:19–21. More generally, “various types of patterns of events can be programmed” into stateful reference monitor 104 for “detection and action.” *Id.* at 9:11–13; *see id.* at 9:13–15.

2. OVERVIEW OF SALAZAR (EXHIBIT 1009)

Salazar is a U.S. patent application publication titled “Method, System, and Program Product for Managing Access to Data Items in a Database,” filed on December 20, 2002, and published on June 24, 2004. Ex. 1009, codes (12), (22), (43), (54). Salazar states that the “invention manages access to data items arranged into a hierarchy of nodes based on access entries associated with the hierarchy of nodes and one or more user properties of an accessing user.” *Id.* ¶ 2; *see id.* ¶¶ 7–11, 19, code (57).

Salazar explains that it is “often desirable to maintain various types of data in a hierarchical structure” to efficiently manage (e.g., locate and retrieve) the data in a relational database. Ex. 1009 ¶¶ 4, 23. Salazar also explains that it is “often desirable to perform access control at an application

level” based on “a user identification or other user property” in a multiuser environment. *Id.* ¶ 5. “Managing access control at this level allows applications to fine-tune the access-control scheme to their needs.” *Id.*

According to Salazar, however, “current application-level implementations require the inclusion of operation-specific data filtering capability at various locations in the application that perform operations on the data stored in the relational database.” Ex. 1009 ¶ 5. Salazar endeavors to address that deficiency by providing a simplified access-control system that “efficiently manages access to data in a relational database above the system level.” *Id.* ¶ 6; *see id.* ¶¶ 7, 19.

Specifically, Salazar discloses managing “access to data items arranged into a hierarchy of nodes” based on “a user property.” Ex. 1009 ¶ 7; *see id.* at code (57). One or more “access entries are associated with the hierarchy of nodes.” *Id.* ¶¶ 7, 19; *see id.* at code (57). “Each access entry associates a user property with an access level.” *Id.* ¶¶ 7, 19; *see id.* at code (57). The “user property is associated with an access level that defines the allowed access to data for that user.” *Id.* ¶¶ 7, 19; *see id.* at code (57). “When an authorized user accesses an application that processes or otherwise provides access to the data, the user is matched with his/her particular user property (e.g., based on log-in information).” *Id.* ¶¶ 7, 19; *see id.* at code (57). “Upon being matched, the particular user property and one or more access entries are used to manage access to the data items.” *Id.* ¶¶ 7, 19.

Salazar explains that “user properties” include “any way of uniquely identifying a set (e.g., one or more) of users,” such as the following:

- “a specific directory expression/path in a hierarchy in which the user(s) are listed”;
- “a group designation of the user(s)”;
- “an attribute of the user(s)”;
- “a ‘group-specific’ property”; and
- “a ‘personal’ property associated with [the] user.”

Ex. 1009 ¶¶ 7, 19, 29; *see id.* ¶ 24. As illustrative “user properties,” Salazar identifies several path/directory expressions derived from a hierarchical directory structure for a plurality of users. *See id.* ¶¶ 24–27.

Salazar’s Figure 2 (reproduced below) depicts an example of a hierarchical directory structure for a plurality of users:

FIG. 2

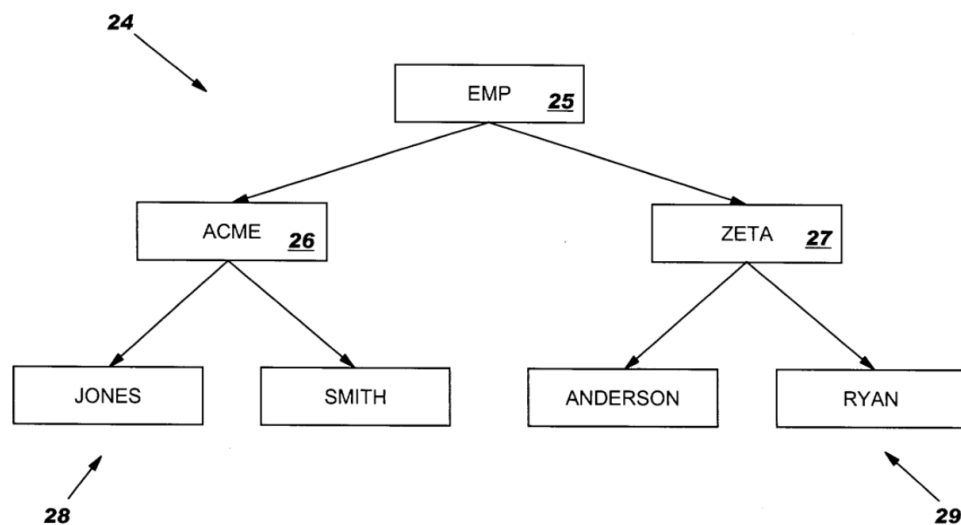


Figure 2 illustrates “hierarchical directory structure 24 for users in an organization” where “EMP directory 25 is the parent directory for all users.” Ex. 1009 ¶ 25, Fig. 2; *see id.* ¶ 14. “Beneath EMP directory 25, ACME directory 26 and ZETA directory 27 are provided for two groups within the organization.” *Id.* ¶ 25, Fig. 2. Personal directories 28 “for users within the

ACME division are located under ACME directory 26,” i.e., personal directories for user Jones and user Smith. *Id.* ¶ 25, Fig. 2. Personal directories 29 “for users within the ZETA division are located under ZETA directory 27,” i.e., personal directories for user Anderson and user Ryan. *Id.* ¶ 25, Fig. 2.

Salazar’s Figure 1 (reproduced below) depicts an example of a hierarchy of nodes:

FIG. 1

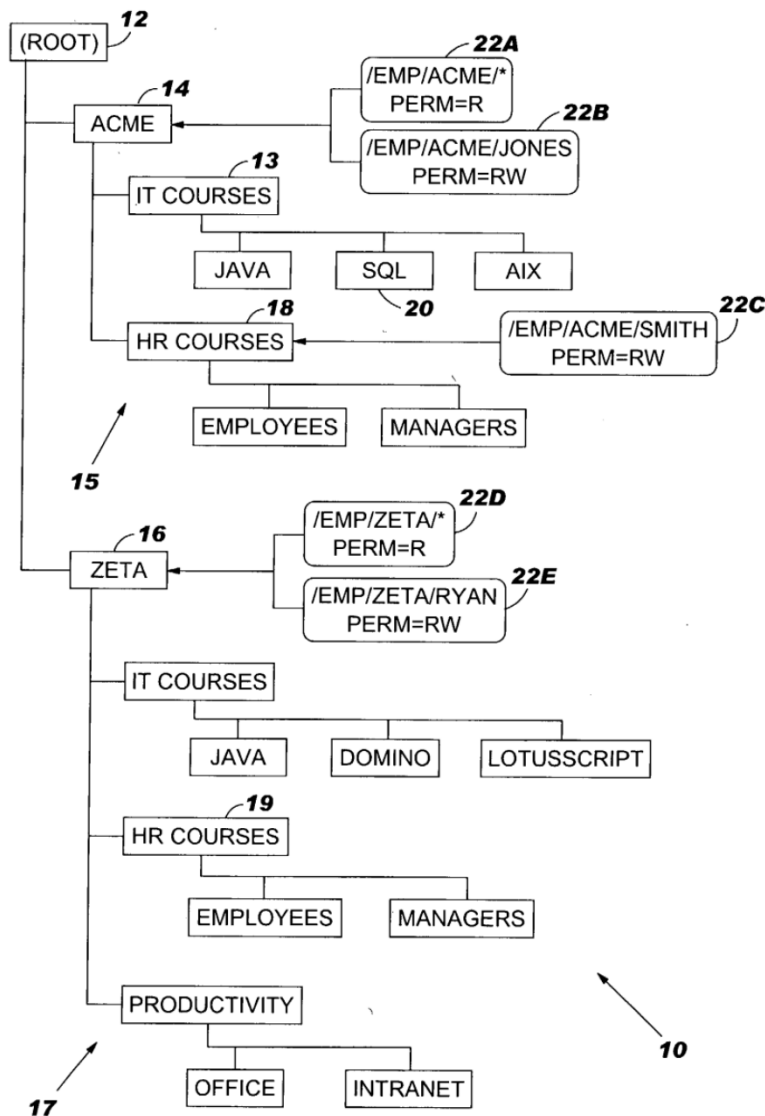


Figure 1 illustrates “a hierarchy of nodes 10” with “a root node 12 at the ‘top’ of the hierarchy.” Ex. 1009 ¶¶ 20–21, Fig. 1; *see id.* ¶ 13. Hierarchy of nodes 10 “shows academic course offerings for two divisions of an organization, ACME and ZETA.” *Id.* ¶ 21, Fig. 1. All “ACME course offerings are categorized according to a hierarchy of nodes 15 under ACME node 14.” *Id.* ¶ 21, Fig. 1. All “ZETA course offerings are categorized according to a hierarchy of nodes 17 under ZETA node 16.” *Id.* ¶ 21, Fig. 1.

Most “data items are typically associated with a node at the lowest level of” hierarchy of nodes 10. Ex. 1009 ¶ 22. For example, “all data items representing courses on the standard query language (SQL) would be associated with SQL node 20” as “one or more child nodes.” *Id.*

To “manage access to the data items, one or more access entries 22A–E are associated with hierarchy of nodes 10.” Ex. 1009 ¶ 24, Fig. 1; *see id.* ¶ 26. Each access entry 22A–E “associates a user property with an access level.” *Id.* ¶ 24, Fig. 1. Specifically, each access entry 22A–E “includes a property string that is based on a user property, and an access level that defines the type of access allowed for a group of users defined by the property string,” such as “read/write” access or “read only” access. *Id.* ¶ 26; *see id.* ¶ 23.

As an example, access entry 22B associates the user property string “/EMP/ACME/JONES” with the access level “PERM=RW” corresponding to “read/write” access for user Jones. Ex. 1009 ¶ 27, Fig. 1. As another example, access entry 22D associates the user property string “/EMP/ZETA/*” with the access level “PERM=R” corresponding to “read only” access for any user with a personal directory under ZETA directory 27, i.e., user Anderson and user Ryan. *Id.* ¶¶ 25, 27, Figs. 1–2. As yet another

example, access entry 22E associates the user property string “/EMP/ZETA/RYAN” with the access level “PERM=RW” corresponding to “read/write” access for user Ryan. *Id.* ¶ 27, Fig. 1.

“Access entries 22A–E and hierarchy of nodes 10 provide the ability to” generate queries that “efficiently return only data items meeting the specified access level for the requesting user, without subsequent filtering to discard inaccessible data items.” Ex. 1009 ¶¶ 19, 28; *see id.* ¶ 7. Hence, “additional filtering of inaccessible data items in the application is not necessary,” thus providing “a more flexible, and efficient implementation of managing access to data items arranged into a hierarchy of nodes.” *Id.* ¶¶ 7, 19, 28.

3. INDEPENDENT CLAIM 1

(a) Preamble

Claim 1 recites “[a] method for secure access to a computer system.” Ex. 1001, 10:16.

Petitioner contends that Gladstone teaches claim 1’s preamble because Gladstone discloses “controlling an operating policy of a computer system, such as a security policy.” Pet. 37 (quoting Ex. 1004, 3:47–48). Further, Petitioner asserts that “Gladstone states that an ‘important aspect of system security is monitoring system events 100, e.g. access requests to a resource, and controlling the effect of those events, e.g. blocking or allowing the requested access to a resource.’” *Id.* (quoting Ex. 1004, 5:6–9).

At this stage of the proceeding, Patent Owner makes no arguments specific to claim 1’s preamble. *See* Prelim. Resp. 1–17. Nonetheless, the burden remains on Petitioner to demonstrate unpatentability. *See Dynamic*

Drinkware, LLC v. Nat'l Graphics, Inc., 800 F.3d 1375, 1378 (Fed. Cir. 2015).

Generally, a preamble does not limit a claim. *Allen Eng'g Corp. v. Bartell Indus., Inc.*, 299 F.3d 1336, 1346 (Fed. Cir. 2002). We need not decide whether claim 1's preamble limits the claim because, based on the current record and for the reasons advanced by Petitioner and supported by Dr. Clark's testimony, Petitioner establishes sufficiently that Gladstone teaches claim 1's preamble. *See* Pet. 37–38; Ex. 1003 ¶¶ 92–94.

(b) Limitation 1a

Limitation 1a recites “receiving in said computer system a request from an entity with a predetermined access level for access to a first base node representing at least one of an information type and a computer system function.” Ex. 1001, 10:18–21 (limitation 1a).

Petitioner contends that the combined disclosures in Gladstone and Salazar teach limitation 1a for several related reasons. *See* Pet. 38–46. First, Petitioner asserts that Gladstone discloses computer system 300 including interceptors 101, stateful reference monitor 104, and a stateless reference monitor. *Id.* at 39–41. Petitioner asserts that interceptors 101 intercept “various types of operating system requests,” called “events,” such as event 100. *Id.* at 39 (emphases omitted) (quoting Ex. 1004, 6:39–40). According to Petitioner, “operating system requests” include “requests for access to operating system resources such as a file or network connection.” *Id.* (emphases omitted) (quoting Ex. 1004, 6:40–42). Petitioner asserts that interceptor 101 intercepts event 100, generates event message 103, and then sends event message 103 to stateful reference monitor 104 for a stateful access decision. *Id.* at 40 (citing Ex. 1004, 5:16–24, 7:25–27, Fig. 1).

Additionally, Petitioner contends that an ordinarily skilled artisan would have understood that “the request for access associated with interception of event 100 and event message 103 would also have been received by Gladstone’s integrated stateless reference monitor for its determination to allow or deny an access request prior to stateful reference monitor 104’s evaluation of that request.” Pet. 41 (emphasis omitted) (citing Ex. 1003 ¶ 96; Ex. 1004, 10:48–52).

For “receiving . . . a request . . . for access” according to limitation 1a, Petitioner identifies each of the following:

- (1) interceptor 101’s intercepting event 100; and
- (2) stateful reference monitor 104’s receiving event message 103.

Pet. 40 (emphases omitted) (citing Ex. 1003 ¶ 95); *see id.* at 41 (citing Ex. 1003 ¶ 96).

For “receiving in said computer system a request . . . for access” according to limitation 1a, Petitioner asserts that (1) interceptor 101’s intercepting event 100 and (2) stateful reference monitor 104’s receiving event message 103 occur in computer system 300. Pet. 41 (emphases omitted) (citing Ex. 1003 ¶ 97; Ex. 1004, 1:64–67).

Second, Petitioner asserts that Gladstone discloses that events 100 include “access requests” for “a number of different resource types,” such as “files, system configuration information, network access, system calls, local or remote object invocation, etc.” Pet. 42 (quoting Ex. 1004, 9:47–50). Petitioner explains that “files” and “system configuration information” exemplify the claimed “information type[s]” and that “network access,” “system calls,” and “local or remote object invocation” exemplify the

claimed “computer system function[s].” *Id.* (alterations by Petitioner) (emphases omitted) (citing Ex. 1003 ¶ 98; Ex. 1004, 6:16, 6:64–7:3, 9:43–55, 10:9–47). Petitioner also asserts that:

- (1) Gladstone’s “different resource types” correspond to “node[s] representing at least one of an information type and a computer system function” according to limitation 1a; and
- (2) “[a]ny of the above requested resources is considered a ‘first’ base node” according to limitation 1a.

Id. at 42–43 (first alteration by Petitioner) (emphases omitted) (quoting Ex. 1001, 10:19–21) (citing Ex. 1003 ¶ 98).

Additionally, Petitioner contends that Gladstone’s disclosure of “nodes” comports with the ’708 patent’s disclosure that “nodes” represent “information access and operational functions for which the security operations are to be enforced.” Pet. 42 (quoting Ex. 1001, 3:64–66) (citing Ex. 1001, 2:67–3:2, 3:46–47; Ex. 1003 ¶ 98).

Third, Petitioner asserts that Gladstone discloses that both a user and a user process may make access requests. Pet. 43 (citing Ex. 1004, 1:64–67, 2:13–20, 6:21–24). Petitioner also asserts that both a user and a user process correspond to “an entity” that makes “a request” according to limitation 1a. *Id.* (citing Ex. 1001, 1:59; Ex. 1003 ¶ 99).

Fourth, Petitioner asserts that Gladstone teaches “a predetermined access level” according to limitation 1a because Gladstone discloses that:

- (1) conventional operating systems include stateless reference monitors that “determine whether a particular access to a file or other resource is permitted”;
- (2) stateless reference monitors make access decisions based on, for instance, (i) “the identity of the user” who makes the request, (ii) “permissions flags,” (iii) “an access

control list associated with the resource,” (iv) “individual permissions [associated] with each user,” (v) “a set of tokens” for “individual users,” and (vi) the “rights and privileges attributed to [a] user”; and

- (3) conventional operating systems “give finer control by associating individual permissions with each user.”

Pet. 43–44 (alterations by Petitioner) (emphases omitted) (quoting Ex. 1004, 2:10–12, 2:17–20, 2:30–31, 2:36–37, 8:2–3) (citing Ex. 1003 ¶ 100).

Fifth, Petitioner asserts that Salazar teaches “a predetermined access level” according to limitation 1a because Salazar discloses that “when a user requests data items and/or attempts to perform an operation on data items, access is allowed, or not, ‘based on one or more particular user properties associated with’” a user that correspond to “a predetermined access level.”

Pet. 44 (emphasis omitted) (quoting Ex. 1009 ¶ 30). Petitioner also asserts that Salazar’s “user properties” are provided to an access-control system that “separately obtains the access entries.” *Id.* According to Petitioner, the access-control system “bases the access determination ‘on the one or more access entries that are matched with [the] user’ using the property associated with the user (a predetermined access level) and the access entry.” *Id.* (alteration by Petitioner) (emphases omitted) (quoting Ex. 1009 ¶ 32) (citing Ex. 1003 ¶ 101; Ex. 1009 ¶¶ 32–34).

Further, Petitioner asserts that Salazar’s “user properties” broadly encompass any property or characteristic that may be associated with a requesting user, such as the following:

- (1) “a path/directory, a group designation, a user attribute, etc.”;
- (2) “a user’s department, country, or role”; and

- (3) a “group specific property or a personal property associated with [the] user.”

Pet. 44–45 (alteration by Petitioner) (emphases omitted) (quoting Ex. 1009 ¶¶ 24, 29) (citing Ex. 1003 ¶ 102; Ex. 1009 ¶ 34).

Sixth, Petitioner asserts that an ordinarily skilled artisan would have understood that “user properties” as broadly disclosed in Salazar include “well-known and widely implemented” properties relating to “security or classification levels,” such as levels used in prior-art access-control systems that compared a user’s predetermined “clearance/authorization,” “security level,” and/or “hierarchical classification” to a “minimum access level.” Pet. 45–46 (emphasis omitted) (citing Ex. 1001, 1:24–27; Ex. 1003 ¶ 103; Ex. 1007, 2:5–9, 2:21–28, 4:23–26, 4:38–51, code (57), Fig. 3; Ex. 1013, 9–10, 60, 65, 111; Ex. 1014 ¶¶ 32–37, 41, Fig. 1; Ex. 1016, 17); *see id.* at 57 (citing Ex. 1003 ¶ 118; Ex. 1007, 2:5–9, 2:21–28, 4:23–26, 4:38–51, code (57), Fig. 3; Ex. 1013, 9–10; Ex. 1014 ¶¶ 32–37, 41, Fig. 1). As support, Petitioner cites, among other things, the disclosure in a 2002 U.S. patent about a “security rank” assigned to users, i.e., “the top rank is A and the rank goes down one by one from A to Z,” that determined whether access to information would be allowed or denied. *Id.* at 45 (citing Ex. 1007, 2:5–9, 2:21–28, 4:23–26, 4:38–51, code (57), Fig. 3).

Seventh, Petitioner asserts that an ordinarily skilled artisan “would have found it obvious to”:

- (1) “combine Salazar’s user properties (a predetermined access level) with Gladstone’s user and user process (both, individually and combined, an entity)”;
- (2) use Salazar’s user properties “in place of Gladstone’s one or more static permissions flags or as part of or in place of an access control list associated with the resource.”

Pet. 46, 54 (emphases omitted) (citing Ex. 1003 ¶¶ 104, 114).

As support for the Gladstone-Salazar combination from the references themselves, Petitioner asserts that both Gladstone and Salazar disclose access-control systems that “provide ‘fine control’ by associating data with each user used in the access control decision.” Pet. 46, 54 (citing Ex. 1004, 2:30–31; Ex. 1009 ¶ 5). Petitioner also asserts that “Salazar states that its fine control is enabled by managing access control at the ‘application level’—the same level at which Gladstone’s stateful reference monitor 104 operates.” *Id.* at 46–47, 54 (citations omitted) (citing Ex. 1004, 6:24–33; Ex. 1009 ¶ 5).

Eighth, Petitioner asserts that an ordinarily skilled artisan “would have understood that Salazar’s user properties” are “predetermined” according to limitation 1a because Salazar discloses that “user properties 40 are ‘set[]’ ‘stored’ and later ‘retriev[ed]’ by various systems.” Pet. 47 (alterations by Petitioner) (citing Ex. 1003 ¶ 105; Ex. 1009 ¶¶ 29, 33).

At this stage of the proceeding, Patent Owner makes no arguments specific to limitation 1a. *See* Prelim. Resp. 1–17.

Based on the current record and for the reasons advanced by Petitioner and supported by Dr. Clark’s testimony, Petitioner establishes sufficiently that the combined disclosures in Gladstone and Salazar teach limitation 1a. *See* Pet. 38–46; Ex. 1003 ¶¶ 95–104, 114.

(c) Limitation 1b

Limitation 1b recites “determining if said access request completes a prohibited temporal access pattern for said entity.” Ex. 1001, 10:22–23 (limitation 1b).

Petitioner contends that Gladstone teaches limitation 1b for several related reasons. *See* Pet. 48–59. First, Petitioner asserts that Gladstone discloses that stateful reference monitor 104:

- (1) observes the “dynamic state” of the computer system using information “collected in real-time, indicative of a condition of a machine or process as a result of a particular sequence of events”;
- (2) tracks a “sequence of actions” to determine whether to allow or deny a request;
- (3) uses a “sequence of actions” to detect “normal behavior” as well as “malicious behavior”; and
- (4) “ensure[s] that requests are ordered, i.e. a request either happens before or after another request.”

Pet. 48–49 (emphases omitted) (quoting Ex. 1004, 2:1–4, 12:22–24, 13:8–10, 13:16–17). According to Petitioner, “various types of patterns of events can be programmed” into stateful reference monitor 104 for “detection and action.” *Id.* at 48 (quoting Ex. 1004, 9:11–13).

Second, Petitioner asserts that Gladstone discloses an example of a “prohibited combination” of events X, Y, and Z (combination X-Y-Z) where stateful reference monitor 104 prohibits event Z if events X and Y have already occurred. Pet. 48 (citing Ex. 1003 ¶ 107; Ex. 1004, 6:13–14).

Third, Petitioner asserts that an ordinarily skilled artisan would have found it obvious for stateful reference monitor 104 to “deny access to event Z if a user requested access because the user had already requested access to event X and/or Y in a particular order.” Pet. 49 (citing Ex. 1003 ¶ 107; Ex. 1004, 12:22–28, 13:8–10).

Fourth, Petitioner asserts that Gladstone teaches “a prohibited temporal access pattern” specific to “said entity” because Gladstone

discloses that a “pattern of events” is “specific to a user and user process.”

Pet. 50. As support, Petitioner quotes Gladstone’s disclosure that “the combination of ‘[e]vents X, Y and Z’ ‘may be’ ‘associated’ ‘with the same user.’” *Id.* (alteration by Petitioner) (quoting Ex. 1004, 6:21–23).

At this stage of the proceeding, Patent Owner makes no arguments specific to limitation 1b. *See* Prelim. Resp. 1–17.

Based on the current record and for the reasons advanced by Petitioner and supported by Dr. Clark’s testimony, Petitioner establishes sufficiently that Gladstone teaches limitation 1b. *See* Pet. 48–50; Ex. 1003 ¶¶ 106–108.

(d) Limitation 1c

Limitation 1c recites “comparing a minimum access level established for said first base node to said predetermined access level.” Ex. 1001, 10:24–25 (limitation 1c).

Petitioner contends that the combined disclosures in Gladstone and Salazar teach limitation 1c. *See* Pet. 52–55. Specifically, Petitioner asserts that Gladstone discloses that:

- (1) a “reference monitor is a component of a computer system that determines whether an access by one component, for example a user process, of another component, for example, a file is permitted”; and
- (2) in “most cases the access decision is made based on”
 - (i) “the identity of the user,”
 - (ii) “one or more static permissions flags or an access control list associated with the resource,” and
 - (iii) matching in the context of access control lists.

Id. at 52, 55 (emphases omitted) (quoting Ex. 1004, 1:64–67, 2:16–20) (citing Ex. 1003 ¶¶ 111, 115).

Additionally, Petitioner asserts that Salazar discloses associating “user properties” with a user and then using “user properties” to “determine whether to grant access.” Pet. 52–53 (citing Ex. 1003 ¶ 112); *see id.* at 44–45 (citing Ex. 1003 ¶¶ 101–102; Ex. 1009 ¶¶ 24, 29–31). According to Petitioner, Salazar also “associates ‘access entries,’ e.g., access entries 22A–E, with various nodes of hierarchy 10 in Figure 1,” and each “access entry 22A–E associates a ‘user property’ with what Salazar describes as an ‘access level.’” *Id.* at 53 (emphasis omitted) (citing Ex. 1009 ¶ 24, Fig. 1).

As an example of how an access entry associates a “user property” with an “access level,” Petitioner identifies access entry 22B in Salazar’s Figure 1 that associates the user property string “/EMP/ACME/JONES” with the access level “PERM=RW” corresponding to “read/write” access for user Jones. Pet. 53 (citing Ex. 1003 ¶ 112; Ex. 1009 ¶ 27, Fig. 1).

Petitioner further asserts that Salazar discloses that “the access control decisions are ‘based on the one or more access entries that are matched with [the] user’ using the property associated with the user and the access entry.” Pet. 55 (alteration by Petitioner) (emphasis omitted) (quoting Ex. 1009 ¶ 32) (citing Ex. 1003 ¶ 115; Ex. 1009 ¶¶ 33–34).

Petitioner explains that an ordinarily skilled artisan “would have found it obvious to use Salazar’s ‘user properties’ in place of Gladstone’s one or more static permissions flags or as part of or in place of an access control list associated with the resource.” Pet. 54 (citing Ex. 1003 ¶ 114); *see id.* at 46 (citing Ex. 1003 ¶ 104).

At this stage of the proceeding, Patent Owner makes no arguments specific to limitation 1c. *See* Prelim. Resp. 1–17.

Based on the current record and for the reasons advanced by Petitioner and supported by Dr. Clark’s testimony, Petitioner establishes sufficiently that the combined disclosures in Gladstone and Salazar teach limitation 1c. *See* Pet. 52–55; Ex. 1003 ¶¶ 110–116.

(e) Limitation 1d

Limitation 1d recites “granting said access request only if it does not complete a prohibited temporal access pattern for said entity, and said minimum access level for said first base node does not exceed said predetermined access level.” Ex. 1001, 10:26–29 (limitation 1d).

Petitioner contends that the combined disclosures in Gladstone and Salazar teach limitation 1d. *See* Pet. 55–58. Specifically, Petitioner asserts that Gladstone discloses that “stateful reference monitor 104 makes a decision” to “block or allow” the last event in a sequence of events for a user or user process. *Id.* at 56 (quoting Ex. 1004, 7:32–35). As support, Petitioner cites Gladstone’s example of a “prohibited combination” of events X, Y, and Z (combination X-Y-Z) where stateful reference monitor 104 prohibits event Z if events X and Y have already occurred. *Id.* (citing Ex. 1004, 6:13–24). Petitioner asserts that an ordinarily skilled artisan would have understood that stateful reference monitor 104 would allow event Z if event Z “did not complete a prohibited temporal access pattern,” e.g., if (1) “the combination of events X-Y-Z were allowed for the user,” (2) “either of events X and Y had not been completed,” or (3) “the events occurred in some other order.” *Id.* (emphasis omitted) (citing Ex. 1003 ¶ 117).

Petitioner asserts that an ordinarily skilled artisan would also have understood that Salazar’s “user properties” include “well-known and widely

implemented” properties relating to “security or classification levels” used in prior-art access-control systems. Pet. 57 (citing Ex. 1003 ¶ 118; Ex. 1007, 2:5–9, 2:21–28, 4:23–26, 4:38–51, code (57), Fig. 3; Ex. 1013, 9–10; Ex. 1014 ¶¶ 32–37, 41, Fig. 1); *see id.* at 14–20. As support, Petitioner cites, among other things, the disclosure in a 2002 U.S. patent about a “security rank” assigned to users, i.e., “the top rank is A and the rank goes down one by one from A to Z,” that determined whether access to information would be allowed or denied. *Id.* at 57 (citing Ex. 1007, 2:5–9, 2:21–28, 4:23–26, 4:38–51, code (57), Fig. 3).

Petitioner further asserts that an ordinarily skilled artisan “would have understood that Gladstone in view of Salazar would allow access when” the user property assigned to the user (corresponding to the claimed “predetermined access level”) meets or exceeds the user property assigned to the resource (corresponding to the claimed “minimum access level for said first base node”). Pet. 56–58 (emphases omitted) (citing Ex. 1003 ¶ 118).

At this stage of the proceeding, Patent Owner makes no arguments specific to limitation 1d. *See* Prelim. Resp. 1–17.

Based on the current record and for the reasons advanced by Petitioner and supported by Dr. Clark’s testimony, Petitioner establishes sufficiently that the combined disclosures in Gladstone and Salazar teach limitation 1d. *See* Pet. 55–58; Ex. 1003 ¶¶ 117–119.

(f) Limitation 1e

Limitation 1e recites “denying said request if said access request completes a prohibited temporal access pattern for said entity.” Ex. 1001, 10:30–31 (limitation 1e).

Petitioner contends that the combined disclosures in Gladstone and Salazar teach limitation 1e for the reasons the combined disclosures teach limitation 1d. *See* Pet. 55–58.

At this stage of the proceeding, Patent Owner makes no arguments specific to limitation 1e. *See* Prelim. Resp. 1–17.

Based on the current record and for the reasons advanced by Petitioner and supported by Dr. Clark’s testimony, Petitioner establishes sufficiently that the combined disclosures in Gladstone and Salazar teach limitation 1e. *See* Pet. 55–58; Ex. 1003 ¶¶ 117–119; *supra* § IV.D.3(e).

(g) Alleged Reason to Combine the Teachings of the References

Petitioner identifies a reason that would have prompted an ordinarily skilled artisan to combine Salazar’s teachings with Gladstone’s teachings in the way Petitioner proposes, e.g., to achieve “more efficient implementation of access control” and improve access-control capability. *See* Pet. 36–37, 46–47, 54, 63–64. Further, Petitioner asserts that an ordinarily skilled artisan “would have had a reasonable expectation of success” in combining the teachings of the references. *Id.* at 47, 54. Dr. Clark’s testimony supports Petitioner’s positions. *See* Ex. 1003 ¶¶ 91, 104, 114, 126.

For instance, Dr. Clark testifies that Salazar discloses that:

- (1) a hierarchy of nodes “is useful in categorizing data items so that they can be efficiently located and retrieved”; and
- (2) associating access entries with the nodes “provides a more flexible, and efficient implementation of managing access to data items arranged into a hierarchy of nodes.”

Ex. 1003 ¶¶ 91, 126 (emphases omitted) (quoting Ex. 1009 ¶¶ 7, 23). He explains that an ordinarily skilled artisan would have recognized that Salazar’s tree structure would have improved the “performance and storage

efficiency” of Gladstone’s access-control system used for “a variety of resources.” *Id.* ¶ 91.

Further, Dr. Clark testifies that Salazar’s access-control system manages access control at “an application level” based on “a user identification or other user property,” and thus “allows applications to fine-tune the access-control scheme to their needs.” Ex. 1003 ¶ 91 (emphases omitted) (quoting Ex. 1009 ¶ 5). He explains that an ordinarily skilled artisan would have recognized that Salazar describes “the details of an example of a stateless reference monitor as described by Gladstone.” *Id.* ¶¶ 104, 114; *see id.* ¶ 91. He also explains that an ordinarily skilled artisan would have recognized that Salazar’s “fine-tuning of access control” would have benefited “Gladstone’s system of implementing access control based on sequences of events at the user level.” *Id.* ¶¶ 91, 104, 114.

At this stage of the proceeding, Patent Owner makes no arguments against combining Salazar’s teachings with Gladstone’s teachings. *See* Prelim. Resp. 1–17.

Based on the current record, Petitioner establishes sufficiently that an ordinarily skilled artisan would have had a reason, e.g., as articulated by Dr. Clark, to combine Salazar’s teachings with Gladstone’s teachings in the way Petitioner proposes. *See* Pet. 36–37, 46–47, 54, 63–64; Ex. 1003 ¶¶ 91, 104, 114, 126. Petitioner also establishes sufficiently that an ordinarily skilled artisan would have had a reasonable expectation of success in combining the teachings of the references. *See* Pet. 47, 54; Ex. 1003 ¶¶ 104, 114.

(h) Preliminary Conclusion About Obviousness/Nonobviousness

As discussed above, Petitioner's analysis addresses how the combined disclosures in Gladstone and Salazar teach claim 1's subject matter. *See supra* §§ IV.D.3(a)–(f). Additionally, Petitioner provides a reason with a rational underpinning as to why an ordinarily skilled artisan would have been motivated to combine Salazar's teachings with Gladstone's teachings in the way Petitioner proposes and would have had a reasonable expectation of success. *See supra* § IV.D.3(g). Hence, Petitioner demonstrates a reasonable likelihood of proving that claim 1 is unpatentable under § 103(a) as obvious over Gladstone and Salazar.

4. DEPENDENT CLAIMS 2–5

Claims 2–5 depend directly or indirectly from claim 1. Ex. 1001, 10:32–52.

For claims 2–5, Petitioner provides an analysis supported by Dr. Clark's testimony about how the combined disclosures in Gladstone and Salazar teach the claimed subject matter. *See* Pet. 59–66; Ex. 1003 ¶¶ 120–131.

At this stage of the proceeding, Patent Owner makes no arguments specific to claims 2–5. *See* Prelim. Resp. 1–17.

Based on the current record and for the reasons advanced by Petitioner and supported by Dr. Clark's testimony, Petitioner establishes sufficiently that the combined disclosures in Gladstone and Salazar teach the subject matter in claims 2–5. *See* Pet. 59–66; Ex. 1003 ¶¶ 120–131. Hence, Petitioner demonstrates a reasonable likelihood of proving that claims 2–5 are unpatentable under § 103(a) as obvious over Gladstone and Salazar.

5. INDEPENDENT CLAIM 9

Claims 1 and 9 recite similar limitations, although their respective preambles differ. *Compare* Ex. 1001, 10:16–31, *with id.* at 11:15–33. Claim 1’s preamble recites “[a] method for secure access to a computer system.” *Id.* at 10:16. Claim 9’s preamble recites “[a] method for restricting access to a computer system having a plurality of logical base nodes representing at least one of an information type and a computer system function, and a plurality of higher-level nodes arranged together with said base nodes in the form of a tree hierarchy.” *Id.* at 11:15–19.

For claim 9, Petitioner provides an analysis supported by Dr. Clark’s testimony about how the combined disclosures in Gladstone and Salazar teach the claimed subject matter. *See* Pet. 67–69; Ex. 1003 ¶¶ 132–138.

At this stage of the proceeding, Patent Owner makes no arguments specific to claim 9. *See* Prelim. Resp. 1–17.

Based on the current record and for the reasons advanced by Petitioner and supported by Dr. Clark’s testimony, Petitioner establishes sufficiently that the combined disclosures in Gladstone and Salazar teach claim 9’s subject matter. *See* Pet. 67–69; Ex. 1003 ¶¶ 132–138. Additionally, as discussed above for claim 1, Petitioner provides a reason with a rational underpinning as to why an ordinarily skilled artisan would have been motivated to combine Salazar’s teachings with Gladstone’s teachings in the way Petitioner proposes and would have had a reasonable expectation of success. *See* Pet. 36–37, 46–47, 54, 63–64; Ex. 1003 ¶¶ 91, 104, 114, 126; *supra* §§ IV.D.3(g)–(h). Hence, Petitioner demonstrates a reasonable likelihood of proving that claim 9 is unpatentable under § 103(a) as obvious over Gladstone and Salazar.

E. Alleged Obviousness over Gladstone, Salazar, and Hada: Claim 6

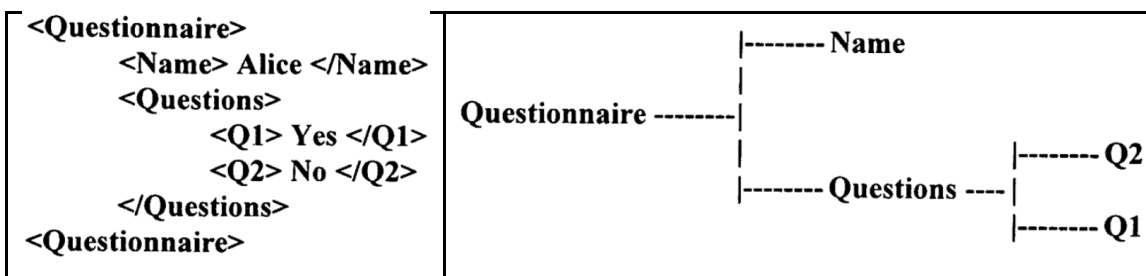
Petitioner contends that claim 6 is unpatentable under § 103(a) as obvious over Gladstone, Salazar, and Hada. *See* Pet. 69–75. Above, we provided overviews of Gladstone and Salazar. *See supra* §§ IV.D.1–IV.D.2. Below, we provide an overview of Hada, and then consider the obviousness issues. As explained below, Petitioner establishes sufficiently for purposes of institution that the combined disclosures in Gladstone, Salazar, and Hada teach claim 6’s subject matter.

1. OVERVIEW OF HADA (EXHIBIT 1005)

Hada is a U.S. patent application publication titled “Method and System for Providing Path-Level Access Control for Structured Documents Stored in a Database,” filed on August 29, 2003, and published on April 7, 2005. Ex. 1005, codes (12), (22), (43), (54). Hada states that the “invention relates generally to computer implemented database systems and, more particularly, to a method and system for providing path-level access control for structured documents stored in a database system.” *Id.* ¶¶ 1, 20; *see id.* at code (57).

Hada explains that a structured document has a “nested” structure and may be represented as “a plurality of nodes forming a hierarchical node tree.” Ex. 1005 ¶¶ 2, 32; *see id.* ¶¶ 5, 21. Each node is “identified by a path that defines a hierarchical relationship between the node and its parent node(s).” *Id.* ¶ 5.

Hada provides the following example of a structured document comprising a questionnaire and its associated node tree:



Ex. 1005 ¶¶ 32–33. Above on the left, the example structured document includes the title “Questionnaire,” the name “Alice,” and the answers to two questions, i.e., “Yes” for question Q1 and “No” for question Q2. *Id.* ¶ 32. Above on the right, the node tree for the example structured document includes a root node identified as “Questionnaire,” two children of the “Questionnaire” root node identified as “Name” and “Questions,” and two children of the “Questions” node identified as “Q1” and “Q2.” *Id.* ¶ 33. Also, the path to node “Q1” is “/Questionnaire/Questions/Q1,” and the path to node “Q2” is “/Questionnaire/Questions/Q2.” *Id.* ¶¶ 33–35.

Hada explains that “Extensible Markup Language (XML)” structured documents are “quickly becoming the standard format for delivering information over the Internet.” Ex. 1005 ¶ 2. As “more and more businesses present and exchange data in XML documents, database management systems (DBMS) have been developed to store, query and retrieve these documents.” *Id.* ¶ 3. Additionally, data security becomes a “crucial concern” when a “collection of documents” is “stored in the database” and “potentially available to large numbers of users.” *Id.* ¶ 4. “In particular, the DBMS must be able to control, i.e., deny or grant, access to the data by the user.” *Id.*

Hada also explains that conventional techniques for controlling access to structured documents include “path-level access control,” i.e., controlling access to each node in a structured document. Ex. 1005 ¶ 5. For instance, “if an administrator wanted to limit access to a ‘salary’ node in all documents in a collection ‘all_employees,’” the administrator would generate a rule to “deny access to all salary nodes with path ‘/employee/salary’ in all documents in [the] collection ‘all_employees.’” *Id.* ¶¶ 6–8. According to Hada, path-level access control becomes “prohibitive” when an access-control policy includes numerous access-control rules. *Id.* ¶ 9.

Hada identifies a need for “an improved method and system for providing path-level access control for structured documents stored in a database.” Ex. 1005 ¶ 10. Hada endeavors to address that need by disclosing the following steps:

- (1) providing an access-control policy comprising a plurality of access-control rules for a collection of structured documents stored in a database;
- (2) “generating a path for each node of the plurality of nodes in” each structured document in the collection;
- (3) “generating for each path associated with a node a corresponding value expression based on at least one” of the access-control rules, where the value expression is a “simple” executable statement “indicating who, if anyone, has access to the node associated with the path”; and
- (4) using the value expression “during access control evaluation to determine whether a user is allowed to access a node in the structured document.”

Id. ¶¶ 10–12, 21, 36, 74, code (57); *see id.* ¶¶ 15, 28–35, Fig. 3. By using value expressions when making access decisions, access-control evaluation and processing are “more efficient and faster” because the value expressions are “less complex” and “easier to process” than an access-control policy comprising a plurality of access-control rules. *Id.* ¶¶ 12, 22, 76.

Each value expression represents a “combination of all” access-control rules affecting the associated node. Ex. 1005 ¶ 36. Preferably, the value expressions are generated by:

- (1) transforming each access-control rule into “a normalized rule format that includes a head, a path expression, and a condition”;
- (2) converting each normalized rule into a modified normalized rule by replacing the condition with a ConditionID corresponding to the condition;
- (3) propagating “each modified normalized rule through each path” in a node tree to determine how an access-control rule “associated with a particular node affects access to ancestor and descendant nodes”;
- (4) combining the modified normalized rules if “more than one modified normalized rule affects a particular path”;
- (5) optimizing the modified normalized rules to “minimize repetitive outputs”; and
- (6) transforming each modified normalized rule into “a value expression for the path” based on the condition expression.

Id. ¶¶ 37–53, 63–66, Fig. 4; *see id.* ¶¶ 54–62.

Propagation has two modes: “up and down.” Ex. 1005 ¶ 43. Propagation-up refers to when an access-control rule “associated with a particular node propagates upward toward its ancestor nodes.” *Id.* Propagation-down refers to when an access-control rule “propagates

downward toward its descendant nodes.” *Id.* “Whether an access control rule propagates up or down depends on a set of propagation rules.” *Id.*

Hada provides the following illustrative propagation rules for a “read” action:

Action	Effect	Mode	Semantics
Read	Grant	Down	Rule specified to any node propagates down.
		Up	Every GRANT for read-access propagates up to all ancestor elements (but not including the attributes and text nodes of these ancestor elements).
	Deny	Down	Rule specified to any node propagates down.
		Up	No propagation

Ex. 1005 ¶ 43.

As an example, if the modified normalized rule associated with a node is a “GRANT read” to user A, “the modified normalized rule propagates up and down from the node,” and user A has “read” access “to all descendant nodes and to all ancestor element nodes.” Ex. 1005 ¶ 45; *see id.* ¶ 43. As another example, if the modified normalized rule associated with a node is a “DENY read” to user B, the modified normalized rule propagates down from the node but does not propagate up, and user B does not have “read” access to any descendant nodes. *See id.* ¶ 43.

According to Hada, “path-level access control prevents the user from gaining access to portions of a document.” Ex. 1005 ¶ 70. “The data to which the user is granted access is displayed, whereas that to which the user is denied access is hidden.” *Id.*

2. DIFFERENCES BETWEEN THE CLAIMED INVENTION AND THE PRIOR ART

Claim 6 depends indirectly from claim 1 and further requires “the step of updating a minimum required entity access level for any base nodes that comprise children of any generation of said higher-level nodes that are aggregations comprising said first base node.” Ex. 1001, 10:53–57.

Petitioner contends that “Gladstone, as modified by Salazar and in view of Hada, renders obvious this step” for several related reasons. *See* Pet. 74–75 (citing Ex. 1003 ¶ 204). First, Petitioner asserts that Gladstone’s “prohibited combination X-Y-Z is an aggregation of” the individual events X, Y, and Z representing base nodes. *Id.* at 74 (citing Ex. 1003 ¶ 204).

Second, Petitioner asserts that an ordinarily skilled artisan would have understood that (1) access to the base nodes represented by the individual events X, Y, and Z and (2) access to the higher-level node represented by the prohibited combination X-Y-Z involves “evaluating Salazar’s user property.” Pet. 74 (citing Ex. 1003 ¶ 204).

Third, Petitioner asserts that an ordinarily skilled artisan would have understood that “it was well known in the art to incorporate higher-access levels for aggregated information.” Pet. 74 (citing Ex. 1001, 6:20–26; Ex. 1003 ¶ 204); *see id.* at 14–20. As support, Petitioner quotes that following explanation from a 1982 book titled “Cryptography and Data Security”: “An aggregate of data might require a higher classification than the individual items. This is because the aggregate might give an overall picture that cannot be deduced (or easily deduced) from an individual item.” *Id.* at 19, 74 (emphases omitted) (quoting Ex. 1016, 17).

Fourth, Petitioner asserts that “Hada discloses ‘propagating’ (updating) the action (e.g., read, update, etc.) and effect (grant, deny) of an access control rule—such as that applied by Gladstone using Salazar’s user properties ‘associated with the resource’ when controlling access to Gladstone’s aggregated node X-Y-Z—down toward ‘descendant[s].’” Pet. 75 (alteration by Petitioner) (emphases omitted) (citing Ex. 1005 ¶ 43). According to Petitioner, an ordinarily skilled artisan “would have found it obvious to incorporate Hada’s teaching into Gladstone, as modified by Salazar,” such that the access-control rules governing aggregated node X-Y-Z would propagate down to the base nodes represented by the individual events X, Y, and Z that correspond to “children of any generation of said higher-level node[]” according to claim 6. *Id.* (emphases omitted) (citing Ex. 1003 ¶ 205).

Fifth, Petitioner asserts that an ordinarily skilled artisan “would have found it obvious to perform this same function multiple times” for “any base nodes that comprise children of any generation of said higher-level nodes” as required by claim 6. Pet. 75 (emphasis omitted) (citing Ex. 1003 ¶ 205).

At this stage of the proceeding, Patent Owner makes no arguments specific to claim 6. *See* Prelim. Resp. 1–17.

Based on the current record and for the reasons advanced by Petitioner and supported by Dr. Clark’s testimony, Petitioner establishes sufficiently that the combined disclosures in Gladstone, Salazar, and Hada teach claim 6’s subject matter. *See* Pet. 73–75; Ex. 1003 ¶¶ 203–205.

3. ALLEGED REASON TO COMBINE THE TEACHINGS OF THE REFERENCES

Petitioner identifies a reason that would have prompted an ordinarily skilled artisan to combine the teachings of Gladstone, Salazar, and Hada. *See* Pet. 73, 75. Dr. Clark’s testimony supports Petitioner’s position. *See* Ex. 1003 ¶¶ 202, 205.

For instance, Dr. Clark testifies that an ordinarily skilled artisan “would have been motivated to implement Hada’s path-level methods in modified-Gladstone to provide ‘more efficient and fast’ access control decisions” for structured documents. Ex. 1003 ¶¶ 202, 205 (quoting Ex. 1005 ¶ 76).

At this stage of the proceeding, Patent Owner makes no arguments against combining the teachings of Gladstone, Salazar, and Hada. *See* Prelim. Resp. 1–17.

Based on the current record, Petitioner establishes sufficiently that an ordinarily skilled artisan would have had a reason, e.g., as articulated by Dr. Clark, to combine the teachings of Gladstone, Salazar, and Hada. *See* Pet. 73, 75; Ex. 1003 ¶¶ 202, 205.

4. PRELIMINARY CONCLUSION ABOUT OBVIOUSNESS/NONOBVIOUSNESS

As discussed above, Petitioner’s analysis addresses how the combined disclosures in Gladstone, Salazar, and Hada teach claim 6’s subject matter. *See supra* § IV.E.2. Additionally, Petitioner provides a reason with a rational underpinning as to why an ordinarily skilled artisan would have been motivated to combine the teachings of Gladstone, Salazar, and Hada. *See supra* § IV.E.3. Hence, Petitioner demonstrates a reasonable likelihood

of proving that claim 6 is unpatentable under § 103(a) as obvious over Gladstone, Salazar, and Hada.

V. CONCLUSION

Based on the arguments and evidence presented by the parties, we determine that there is a reasonable likelihood Petitioner would prevail with respect to at least one claim challenged in the Petition. Hence, we institute an *inter partes* review of all challenged claims on all challenges included in the Petition. *See SAS Inst. Inc. v. Iancu*, 138 S. Ct. 1348, 1355 (2018) (noting that the language of 35 U.S.C. § 314(b) “indicates a binary choice—either institute review or don’t”); *PGS Geophysical AS v. Iancu*, 891 F.3d 1354, 1360 (Fed. Cir. 2018) (interpreting the statute as requiring “a simple yes-or-no institution choice respecting a petition, embracing all challenges included in the petition”). Additionally, we decline to exercise our discretion under § 314(a) to deny institution.

At this preliminary stage, we have not made a final determination about the patentability of any challenged claim, the construction of any claim term, phrase, or limitation, or any other legal or factual issue.

VI. ORDER

Accordingly, it is

ORDERED that, pursuant to 35 U.S.C. § 314(a), an *inter partes* review of claims 1–6 and 9 in the ’708 patent is instituted on all challenges included in the Petition; and

FURTHER ORDERED that, according to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, notice is hereby given of the institution of a trial that commences on the entry date of this decision.

IPR2023-00669
Patent 7,302,708 B2

For PETITIONER:

Monté T. Squire
Patrick D. McPherson
Paul H. Belnap
DUANE MORRIS LLP
MTSquire@duanemorris.com
PDMcPherson@duanemorris.com
PHBelnap@duanemorris.com

For PATENT OWNER:

Brett E. Cooper
BC LAW GROUP, P.C.
bcooper@bc-lawgroup.com
Lionra_Counsel@b-clg.com

Robert A. Auchter
AUCHTER PLLC
robert@auchterlaw.com