

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ORCA SECURITY LTD.,
Petitioner,

v.

WIZ, INC.,
Patent Owner.

IPR2025-01087
U.S. Patent No. 12,003,529

Before KARL D. EASTHOM, NABEEL U. KHAN, and LISA A.
MURRAY, *Administrative Patent Judges*.

MURRAY, *Administrative Patent Judge*.

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

I. INTRODUCTION

A. Background and Summary

Orca Security Ltd. (“Petitioner”) filed a Petition (Paper 1, “Pet.”) requesting institution of *inter partes* review of claims 1–17 of U.S. Patent No. 12,003,529 (“the ’529 Patent”). Wiz, Inc. (“Patent Owner”) filed a Preliminary Response (Paper 9, “Prelim. Resp.”). With the authorization of the Board, Petitioner filed a Preliminary Reply (Paper 11, “Prelim. Reply”), and Patent Owner filed a Preliminary Sur-Reply (Paper 12, “Prelim. Sur-Reply”).¹

An *inter partes* review may be instituted only if “the information presented in the petition . . . and any [preliminary] response . . . shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” 35 U.S.C. § 314(a). For the reasons given below, on this record, Petitioner has established a reasonable likelihood that it would prevail in showing the unpatentability of at least one of the challenged claims. We determine that institution of an *inter partes* review of the challenged claims is appropriate.

B. Real Parties in Interest

Petitioner identifies Orca Security Ltd. as a real party in interest. Pet. 54. Patent Owner identifies Wiz., Inc. as a real party in interest. Paper 3, 1 (Patent Owner’s Mandatory Notices).

¹ Patent Owner also filed a Request for Discretionary Denial (Paper 7). Petitioner filed an Opposition to Patent Owner’s Request for Discretionary Denial (Paper 8). On October 17, 2025, an Order issued denying Patent Owner’s Request for Discretionary Denial and referring the matter to this Panel for consideration. Paper 10.

C. Related Matters

The parties identify the following pending litigation involving the '529 Patent: *Orca Security Ltd. v. Wiz, Inc.*, No. 1:23CV-00758 (D. Del.). Pet. 54; Paper 3, 1.

D. The '529 Patent

The '529 Patent issued on June 4, 2024 and is entitled “Techniques for detecting artificial intelligence model cybersecurity risk in a computing environment.” It relates to U.S. App. No. 18/584,659 (filed Feb. 22, 2024). Ex. 1001, codes (21), (22). The '529 Patent claims “[a] system and method for detecting a cybersecurity risk of an artificial intelligence (“AI”).” The method includes: inspecting a computing environment for an AI model deployed therein; generating a representation of the AI model in a security database that includes “a representation of the computing environment; inspecting the AI model for a cybersecurity risk; generating a representation of the cybersecurity risk in the security database;” and “initiating a mitigation action based on the cybersecurity risk.” *See* Ex. 1001 code (57).

E. Illustrative Claim

Petitioner challenges claims 1–17. The independent claims are claim 1, a method claim, claim 9, which claims a non-transitory computer-readable medium, and claim 10, a system claim. Claims 9 and 10 are similar in scope to claim 1. *Compare* Ex. 1001, 19:23–37, *with id.* at 19:60–20:11. Claim 1, reproduced below with Petitioner’s bracketed identifiers added (*see, e.g.*, Pet. 56–58), is representative of the challenged claims:

1.[1[P]] A method for detecting a cybersecurity risk of an artificial intelligence (AI), comprising:

[1[a]] generating an inspectable disk based on an original disk of a resource deployed in a computing environment;

[1[b]] inspecting the inspectable disk for an AI model;

[1[c]] generating a representation of the AI model in *a security database*, the security database including a representation of the computing environment;

[1[d]] inspecting the AI model for a cybersecurity risk;

[1[e]]² generating a representation of the cybersecurity risk in the security database, the representation of the cybersecurity risk connected to the representation of the AI model in response to detecting the cybersecurity risk; and

initiating a mitigation action based on the cybersecurity risk.

Ex. 1001 at 19:23–37 (*emphasis* added to disputed term); Pet. 56.

F. Evidence

Petitioner relies on the following patent evidence:

Name	Patent Document	Exhibit
Shua ³	US 11,489,863 B1	1004
Lang	US 2024/0202405 A1	1006

Pet. 6. Petitioner also relies on a Declaration of Erez Zadok in support of the Petition. Ex. 1003.

² Petitioner’s claim appendix labels the last limitation of claim 1 as “1[e]”, but both parties refer to the second-to-last limitation as “1[e]” in their briefs.

³ Petitioner relies on both the Shua issued patent (Ex. 1004, “Shua”) and the corresponding provisional, US Prov. App. No. 63/180,048 (Ex. 1005, “Shua ’048”). The contents of Shua ’048 are incorporated by reference in their entirety in the issued patent. Ex. 1004, 1:5–16. Petitioner asserts that the disclosures of Shua ’048 are “as much a part of the application as filed as if the text was repeated in the application, and should be treated as part of the text of the application as filed.” Pet. 7 (citing MPEP § 2163.07(b)). Petitioner states that consequently the Petition “relies on the disclosures of Shua and the Shua Provisional as a single prior art reference.” *Id.*; *see* discussion in Section II.E.1 below.

G. Prior Art and Asserted Grounds

Petitioner asserts that claims 1–17 would have been unpatentable on the following ground:

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1–17	103	Shua, Lang

Pet. 6.

II. ANALYSIS

A. Legal Standards

An invention is not patentable if “the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains.” 35 U.S.C. § 103. The question of obviousness is resolved on the basis of underlying factual determinations including (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and, (4) where in evidence, so-called secondary considerations, including commercial success, long-felt but unsolved needs, and failure of others.⁴ *Graham v. John Deere Co. of Kansas City*, 383 U.S. 1, 17–18 (1966).

⁴ At this stage, neither party has directed us to evidence of such secondary considerations. The ultimate legal determination of whether the claimed combination would have been obvious to an ordinary artisan would depend on several factors, including objective evidence of nonobviousness, if present. *Arctic Cat Inc. v. Bombardier Recreational Prods. Inc.*, 876 F.3d 1350, 1361 (Fed. Cir. 2017); *Graham*, 383 U.S. at 17–18.

When evaluating a combination of teachings,

[o]ften, it will be necessary for a court to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine 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) (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)). Moreover, “[w]here a party argues a skilled artisan would have been motivated to combine references, it must show the artisan would have had a reasonable expectation of success from doing so.” *Arctic Cat*, 876 F.3d at 1360–61 (internal punctuation omitted).

B. Level of Ordinary Skill in the Art

Determining whether an invention would have been obvious under 35 U.S.C. § 103 involves determining the level of ordinary skill in the pertinent art at the time the invention was made. *Graham*, 383 U.S. at 17. The level of skill in the art is “a prism or lens” through which we view the prior art and the claimed invention. *Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001). The person of ordinary skill in the art is a hypothetical person who knows the relevant art. *In re GPAC Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995). Factors to consider include the types of problems encountered in the art, the sophistication of the technology, and the educational level of active workers in the field. *Id.* One or more factors may predominate. *Id.*

Petitioner asserts that one of ordinary skill in the field of the ’529 Patent would have had “a bachelor’s degree in computer engineering, computer science, electrical engineering, or a similar degree, with 2–3 years

of experience in the fields of cybersecurity and artificial intelligence; additional education or experience might substitute for these requirements.”

Pet. 5; Ex. 1003 ¶¶ 32–33. Patent Owner’s Preliminary Response does not address this issue. We find Petitioner’s formulation to be consistent with the evidence of record at this stage of the proceedings, including the asserted prior art and the ’529 Patent, and we preliminarily adopt and apply that definition for purposes of this Decision.

C. Claim Construction

We interpret claims in the same manner used “in a civil action under 35 U.S.C. § 282(b), including construing the claim in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.” 37 C.F.R. § 42.100(b). When applying that standard, we interpret the claim language as it would have been understood by one of ordinary skill in the art in light of the specification. *Wasica Fin. GmbH v. Cont’l Auto. Sys., Inc.*, 853 F.3d 1272, 1279–80 (Fed. Cir. 2017). Thus, we give claim terms their ordinary and customary meaning as understood by an ordinarily skilled artisan. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005) (en banc).

Petitioner states that in the related district court litigation identified above, the parties have not identified any claims as requiring construction. Pet. 6. Petitioner argues that no claim terms require construction to determine the validity of the challenged claims under Petitioner’s proposed grounds of unpatentability. *Id.* Patent Owner’s Preliminary Response does not address this issue.

After reviewing the parties' arguments and the evidence presented, we determine that to render our Decision we will need at least a preliminary understanding of the meaning of the term "security database" in limitation 1[c] of the '529 Patent (and in the corresponding limitations in claims 9 and 10). We discuss our initial conclusions in Section E.2.a below. Our preliminary analysis is based on the current record and may change after the record is developed during trial. The parties are encouraged to address the proper construction of the term "security database" in future briefing.

D. Scope and Content of the Prior Art

1. Shua (Exs. 1004, 1005)

Shua was filed on April 8, 2022, claiming priority to Shua '048, filed on April 26, 2021. Ex. 1004, codes (22), (60). Shua issued on November 1, 2022. *Id.* code (45). Petitioner asserts that therefore under 35 U.S.C. §§ 102(a)(1) and (2) Shua qualifies as prior art to the '529 Patent, which was filed on February 22, 2024. Pet. 7.

The issued Shua patent is entitled "Foundation of SideScanning." Ex. 1004, code (54). Shua discloses techniques for detecting risk across all of an organization's assets in a cloud environment. It addresses a need for improved security scanning systems that are more adapted for use in cloud infrastructures. Ex. 1004, 2:66–3:7. Shua discloses that its techniques help organizations to: "(1) Detect risks such as vulnerabilities, malware, misconfigurations, lateral movement risk, and unsecured sensitive data; (2) See cloud inventory at every layer: infrastructure, operating system, applications, and data; (3) Discover and see previously missed assets." *Id.* at 3:2–7. The techniques include a scanning system 101 that may generate a map of cloud infrastructure 106. *Id.* at 9:53–64; 13:1–5. In some

embodiments, this map may be in a form of a graph: a plurality of interconnected vectors connecting a plurality of systems and devices, based on the networking configuration. *Id.* at 13:1–5. Upon gathering network accessibility information and identifying one or more vulnerabilities susceptible to external attack, “a disclosed embodiment would have the functionality to perform processes to gather, display, and mitigate a discovered vulnerability.” *Id.* at 24:61–66; *see also id.* at 30:31–33 (“The scanning system 101 may be able to access and identify software vulnerabilities for mitigation, rectification, correction, and fortification.”).

The title of the Shua ’048 provisional is “Cloud Cybersecurity.” Ex. 1005, 1. As noted above, the issued Shua patent incorporates all of the disclosures of Shua ’048 by reference. Ex. 1004, 1:6–16. Like the issued Shua patent, Shua ’048 discloses “[a] system for generating a composite cybersecurity risk assessment in a cloud environment.” Ex. 1005, 57 (exemplary independent claim). Specifically, Shua ’048 describes Orca Security, a system that:

delivers instant-on, work-load level visibility across 100% of AWS, Azure, and GCP assets without running a single opcode in the customer environment, helping organizations to: (1) Detect risks such as vulnerabilities, malware, misconfigurations, lateral movement risk, and unsecured sensitive data; (2) See cloud inventory at every layer: I/S, OS, applications, and data; (3) Discover and see previously missed assets.

Ex. 1005 ¶ 14.

Shua ’048 discloses that “Orca may provide deep and contextualized visibility of cloud environments. It covers 100% of an organization’s assets.” Ex. 1005 ¶ 29; *see id.* ¶ 39. “After a customer adds an account to Orca, the SideScanning™ process starts with building a map of the

customer's organization's entire estate.” *Id.* ¶ 35. It “visualize[s] and build[s] a map of a customer's entire environment.” *Id.* ¶ 33.

Orca “scans the configuration, network layout, and security configuration” of a cloud environment while also “reading into virtual machines, disks, databases, and datastores, as well as logs for cloud assets. It then analyzes the data and builds a full-stack inventory. Next it automatically assesses the security state of discovered asset[s] throughout the technology stack, including all four cloud layers: I/S, OS, apps, and data.” Ex. 1005 ¶ 30. “Every asset in the account may be enumerated in all regions (e.g., geographic locations). . . .” *Id.* ¶ 35.

After mapping an organization's cloud-based assets, Orca matches those assets to known vulnerabilities in its vulnerability database. Ex. 1005 ¶ 42. It takes the asset map and enriches this information with the risk data. *Id.* ¶¶ 61, 64 (graphic). Finally, Shua '048 discloses that “[s]uch analysis may be presented to a user via [a] graphical user interface.” *Id.* ¶ 61.

2. *Lang (Ex. 1006)*

Lang teaches a “[m]ethod and system for analyzing a computing system for properties of a machine learning model in the computing system[.]” Ex. 1006, code (57). Lang explains that “it is difficult to ensure AI systems are working as intended, and they are difficult to audit.” Ex. 1006 ¶ 6. Lang further states that AI systems “may be prone to adversarial attacks, wherein an attack manipulates the AI model or data (incl. training or inference data) in a way that affects the model's behavior and decision-making.” *Id.* Thus, “[t]here is a need for better mechanisms and tools that ensure AI systems are . . . safe, and secure.” *Id.*

Lang uses “surrogate model analysis and explainability techniques to determine weaknesses, vulnerabilities, anomalies, and errors with the system and, for example, to automatically harden the system to mitigate them[.]”

Ex. 1006 ¶ 21. This includes “detecting and/or analyzing AI components in virtual machines and containerized and virtual environments.” *Id.* ¶ 30. “AI and/or characteristics of AI, may be detected in computing systems by analyzing for example inputs and outputs.” *Id.* ¶ 32. “[M]onitoring may include continuously analyzing the AI systems 105 for vulnerabilities. If vulnerabilities are discovered, then a hardening action may be used to harden the system against those vulnerabilities.” *Id.* ¶ 122.

3. Motivation to Combine

Petitioner argues that one of ordinary skill in the relevant art would have been motivated to modify the “system for generating a composite cybersecurity risk assessment in a cloud environment” taught in Shua (Ex. 1005, 57) by incorporating Lang’s “system for analyzing a computing system for properties of a machine learning model in the computing system” (Ex. 1006, code (57)). Pet. 10–11; Ex. 1003 ¶¶ 82–84. Dr. Zadok testifies that the combined Shua- Lang system would detect cybersecurity risks in artificial intelligence (“AI”) systems. Ex. 1003 ¶ 82.

Petitioner argues that Shua provides an express motivation to combine the two references by teaching that it is desirable to scan “100% of an organization’s assets.” Pet. 11. Also, Petitioner contends that it would have been desirable to scan Lang’s artificial intelligence models to detect any cybersecurity risks present therein. *Id.* at 12. Petitioner further contends that the combination would have constituted the use of a known technique (Lang’s scanning of AI models) to improve a similar device (Shua’s system

for scanning an organization's assets) in the same way, and would have required only minor modifications to software. *Id.*

E. Ground 1: Obviousness over Shua (Exs. 1004, 1005) and Lang (Ex. 1006)

Petitioner asserts that claims 1–17 are unpatentable as obvious over the combination of Shua and Lang. Pet. 10–52. Patent Owner argues that the Shua provisional, Shua '048, is not prior art and cannot be relied upon in these proceedings. Prelim. Resp. 2–6. Patent Owner also argues that Petitioner has not established that the proposed combination of prior art discloses elements 1[c] or 1[e] of representative claim 1. *Id.* at 6–16. Finally, Patent Owner argues that the Petition does not demonstrate a reasonable expectation of success in making the proposed combination. *Id.* at 16–17. We determine that Petitioner has demonstrated a reasonable likelihood of prevailing on at least one challenged claim and that Patent Owner's arguments do not rebut Petitioner's showing at this stage of the proceeding for the reasons discussed below.

1. Whether Petitioner May Rely on Shua '048 in These Proceedings

Patent Owner's first argument is that Petitioner expressly relies on both the Shua patent and the Shua provisional application as ground references and that this is improper because the provisional Shua '048 itself purportedly cannot be a basis for an *inter partes* review. Prelim. Resp. 2–6; (citing 35 U.S.C. § 311(b); 37 C.F.R. § 42.104(b)(2)).

a. Incorporation by Reference

Patent Owner is correct that Shua '048, if it had not been incorporated into the public file history of the Shua patent, could not have been a basis for an *inter partes* review because provisional applications, standing alone, are

neither patents nor printed publications. 35 U.S.C. § 311(b). That is not, however, how Petitioner has used the reference. The issued Shua patent expressly states that “[t]his application claims the benefit of U.S. Provisional Application No. 63/180,048 filed on Apr. 26, 2021, the contents of which are hereby incorporated by reference.”⁵ Ex. 1004, 1:14–16. This is a permissible practice. MPEP § 608.01(p)(I)(A) (“An application as filed must be complete in itself in order to comply with 35 U.S.C. 112. Material nevertheless may be incorporated by reference.”). Petitioner asserts that the disclosures of Shua ’048 are “as much a part of the application as filed as if the text was repeated in the application,” and that accordingly Petitioner relies on the disclosures of the issued Shua patent and the Shua ’048 provisional “as a single prior art reference.” Pet. 7. (citing MPEP § 2163.07(b)). In other words, Shua ’048 is not a separate ground reference; it is cited as evidence of the content of the issued Shua patent, which as a patent indisputably qualifies as prior art usable in an *inter partes* review. 35 U.S.C. § 311(b). The issued Shua patent is the prior art reference; the Shua ’048 provisional published as part of the patent’s file history is evidence of what that patent discloses.

In support of its position, Petitioner cites to MPEP § 2163.07(b), which provides in relevant part:

Instead of repeating some information contained in another document, an application may attempt to incorporate the content of another document or part thereof by reference to the document

⁵ Shua repeats this assertion, stating that “[t]his application is a continuation of PCT International Application No. PCT/IB2022/052670, filed Mar. 23, 2022, which claims the benefit of U.S. Provisional Application No. 63/180,048 filed Apr. 26, 2021, the contents of each of which are hereby incorporated by reference in their entireties.” Ex. 1004, 1:6–10.

in the text of the specification. *The information incorporated is as much a part of the application as filed as if the text was repeated in the application, and should be treated as part of the text of the application as filed.*

MPEP § 2163.07(b) (emphasis added). While Patent Owner argues that this provision merely “discusses how to fix a new-matter problem in an application under examination,” (Prelim. Resp. 3), the provision does more than this; it refers the reader to MPEP § 608.01(p), quoted above, for Office policy regarding incorporation by reference. MPEP § 2163.07(b). The provision also cites to 37 C.F.R. § 1.57, the relevant portion of which reads:

(c) Except as provided in paragraph (a) or (b) of this section, an incorporation by reference must be set forth in the specification and must:

- (1) Express a clear intent to incorporate by reference by using the root words “incorporat(e)” and “reference” (*e.g.*, “incorporate by reference”); and
- (2) Clearly identify the referenced patent, application, or publication.

37 C.F.R. § 1.57(c). The Shua patent complies with these requirements. *See* Ex. 1004, 1:5–16. Thus, Shua ’048 is as much a part of the application that became the issued Shua patent as if its text were repeated in the application.

Documents that incorporate material by reference may be used as prior art and the incorporated material may be considered, even in an anticipation context. *Advanced Display Sys., Inc. v. Kent State Univ.*, 212 F.3d 1272, 1282 (Fed. Cir. 2000) (anticipation context). This is equally true for provisional applications that become publicly available due to their incorporation into a published patent or patent application. *See, e.g., Konda v. Flex Logix Techs., Inc.*, 2022 WL 1436144 (Fed. Cir. May 6, 2022) (affirming Board decision that a provisional application incorporated by

reference into a PCT application was prior art “by virtue of the fact that it became publicly available due to its incorporation into the ’756 PCT, and in addition is prior art because it is part of the ’756 PCT itself.”).

b. In re Arkley

Patent Owner argues that “[e]ven if Petitioner’s use of the Shua ’048 provisional application as part of the Shua ’863 patent disclosure were appropriate, it would still present an *In re Arkley* problem.” Prelim. Resp. 5 (citing *In re Arkley*, 455 F.2d 586, 587–588 (CCPA 1972)). *In re Arkley* held that an anticipation rejection was improper because the prior art reference did not “clearly and unequivocally disclose the claimed compound or direct those skilled in the art to the compound without *any* need for picking, choosing, and combining various disclosures not directly related to each other by the teachings of the cited reference.” *In re Arkley*, 455 F.2d at 587; *see also Net MoneyIN, Inc. v. VeriSign, Inc.*, 545 F.3d 1359, 1371 (Fed. Cir. 2008) (In an anticipation context, “it is not enough that the prior art reference . . . includes multiple, distinct teachings that [an ordinary] artisan might somehow combine to achieve the claimed invention.”).

Neither *In re Arkley* nor *Net MoneyIN* is relevant to this obviousness challenge. *In re Arkley* expressly states that while “picking, choosing, and combining various disclosures not directly related to each other” has no place in an anticipation context, “[s]uch picking and choosing may be entirely proper in the making of a 103, obviousness rejection[.]” *In re Arkley*, 455 F.2d at 587–588. Thus, Petitioner’s use of Shua ’048 in an obviousness challenge does not “present a problem” under *In re Arkley*.

Moreover, the evidence does not support Patent Owner’s overall argument that Petitioner is combining teachings from “two very different

disclosures . . . without providing any analysis regarding motivation to combine the different disclosures’ teachings or reasonable expectation that the combination would succeed.” Prelim. Resp. 5–6. According to Patent Owner, “simple comparison shows the Shua’863 patent and Shua’048 provisional application disclosures are very different, including very different figures[.]” *Id.* at 6. Petitioner counters that “Shua’s disclosures are facially a development of the Shua Provisional’s technology, describing substantially the same concepts: both the Shua and Shua Provisional Background and ‘disclosed embodiments’ are in common.” Prelim. Reply 3 (comparing Ex. 1005 ¶ 1 *with* Ex. 1004, 1:33–42 (describing the technical field in virtually identical language) *and* Ex. 1005, 45–72 *with* Ex. 1004, 78:27–84:10 (disclosing substantially similar exemplary claims)).

We find a “simple comparison” shows that Patent Owner’s argument is not supported by the evidence. Shua ’048 describes the operation of a novel Orca Security product called SideScanning™.⁶ *E.g.*, Ex. 1005 ¶ 29. The issued Shua patent, which is *entitled* “Foundation of SideScanning,” teaches the same technology.⁷ *See, e.g.*, Ex. 1004, 6:40–51. The various

⁶ Specifically, Shua ’048 teaches that “SideScanning is a radical approach because Orca does not necessarily go *inside* each workload to inspect data. Instead, it uses an out-of-band process to reach cloud workloads through the runtime storage layer, combining this with metadata gathered from cloud provider APIs. Orca may provide deep and contextualized visibility of cloud environments. It covers 100% of an organization’s assets with[out] necessarily needing an agent or network scanner.” Ex. 1005 ¶ 29.

⁷ The issued patent’s description of this technology is very similar to the description in Shua ’048: “Embodiments of the present disclosure include technology referred to as “SideScanning.” In contrast to some existing systems and techniques, these embodiments may provide a distinct advantage because the technology does not necessarily require entering into each workload to inspect data. Rather, some embodiments use an out-of-

disclosures of the Shua patent and Shua '048 are in fact “directly related to each other.” *Cf. In re Arkley*, 455 F.2d at 587. Thus, even if the caselaw cited by Patent Owner were applicable in this obviousness challenge, Patent Owner’s argument would still be factually deficient.

2. Whether Petitioner Has Shown that the Proposed Combination Discloses Each Limitation of the Challenged Claims

Patent Owner next argues that Petitioner has not shown that the proposed combination of prior art discloses limitations 1[c] and 1[e] of independent claim 1. Prelim. Resp. 6–16. Patent Owner does not dispute any other aspect of Petitioner’s mapping of the proposed prior art combination to the challenged claims. We have conducted an independent review of the claim mapping set forth in the Petition, and we conclude that Petitioner has provided “[a] full statement of the reasons for the relief requested, including a detailed explanation of the significance of the evidence.” *See* 37 C.F.R. § 42.22(a)(2). We find Petitioner’s analysis of the challenged independent claims to be consistent with the evidence of record at this stage of the proceeding, including the asserted prior art and the Declaration of Erez Zadok (Ex. 1003). We explain our reasons for reaching this conclusion for disputed limitations 1[c] and 1[e] in the discussion that follows below.

a. Independent Claims 1, 9, and 10: Limitation 1[c]

Limitation 1[c] reads, “generating a representation of the AI model in a security database, the security database including a representation of the

band process to reach cloud workloads through a runtime storage layer, combining this with metadata gathered from API provided through a cloud service provider's system, thus providing visibility of cloud environments both at a low level and with context, without the requirement for an agent or network scanner.” Ex. 1004, 6:40–51.

computing environment.” Ex. 1001, 19:28–30. The same limitation appears in independent claims 9 and 10. *Id.* at 20:1–3, 20:23–25. Petitioner argues that Shua in view of Lang teaches this limitation. Pet. 17–21. Patent Owner argues that Petitioner’s 1[c] analysis at best describes “a stored graph representation of a computer environment,” and fails to identify the recited “security database” in the prior art. Prelim. Resp. 7–8.

i. Preliminary claim construction: “security database”

Although the parties argue that no express claim construction is necessary for purposes of this Decision, they appear to dispute the proper scope of the term “security database.” Petitioner argues that “[t]he ’529 Patent gives as an example of a security database, a ‘graph database, such as Neo4j®.’”⁸ Pet. 17; Ex. 1001, 7:58–60. The ’529 Patent explains that “[i]n an embodiment, a security database is implemented as a graph database, based on a unified data schema. In some embodiments, the security database includes a plurality of nodes and connections between the nodes.”⁹ Ex. 1001, 8:36–39; *see also id.* at 4:1–3, Fig. 2 (depicting “an example security graph representation of an AI pipeline”). According to Petitioner’s witness, Dr. Zadok, “[a] POSITA would have understood that the term ‘security

⁸ Petitioner’s witness, Dr. Zadok, explains that a POSITA would have understood that a graph database is “a form of stored data structure where (1) entities are represented as ‘nodes,’ (2) connections and/or relationships between entities are represented by ‘edges’ connecting the nodes, and (3) properties of nodes and edges are represented by ‘attributes’ attached to the nodes and edges.” Ex. 1003 ¶ 100.

⁹ The ’529 Patent provides that a security database may also be implemented as “a columnar database, a SQL database[,] a non-SQL database, a table, a plurality of tables, a graph database, combinations thereof, and the like.” Ex. 1001, 7:55–58.

database’ in the ’529 Patent encompassed a stored data structure representing the computing environment as nodes, edges, and attributes.” Ex. 1003 ¶ 100. Petitioner argues that “[t]hus, in the terms of the ’529 Patent, a stored representation of the computing environment as nodes, edges, and attributes of nodes and edges is a *security database including a representation of the computing environment*.” Pet. 17.

Patent Owner objects to this interpretation of limitation 1[c]. Patent Owner contends that Petitioner’s argument “inverts the appropriate understanding: just because the challenged patent identifies an example security database that stores a representation of a computing environment as nodes and edges does not mean that anything that stores a representation of a computing environment as nodes and edges is necessarily a security database.” Prelim. Resp. at 7–8. We agree with the logic of Patent Owner’s argument, but disagree that Petitioner necessarily “relies on this inverted understanding for its prior art mapping.” *Id.* at 8. We understand Dr. Zadok’s explanation to mean only that the claim term “security database” *encompasses* graph databases that include a representation of the computing environment, meaning that some (but not necessarily all) security databases are graph databases. *See* Ex. 1003 ¶ 100. The language in the Petition to which Patent Owner objects can be read consistently with Dr. Zadok’s declaration. Petitioner does not, however, take a position on what the outer bounds of the claim term “security database” should be.

Without attempting a full construction of the term “security database,” it is possible to determine from the current record, at least on a preliminary basis, some of the database types that would fall within its scope. The ’529 Patent explains that the claimed “security database” is part of an “inspection

environment 130” that monitors the computing environment for cybersecurity threats. Specifically, it provides as follows:

In certain embodiments, the cloud computing environment 110 is monitored for cybersecurity objects, threats, risks, and the like, by an inspection environment 130. In an embodiment, the inspection environment 130 is configured to monitor the cloud computing environment 110 for cybersecurity objects, threats, risks, combinations thereof, and the like.

Ex. 1001, 6:1–7; *see id.* Fig. 1. The ’529 Patent also provides: “In an embodiment, the inspection environment 130 further includes a security database 136. In some embodiments, the security database 136 is configured to store a representation of the cloud computing environment 110, for example based on a predetermined data schema.” *Id.* at 7:46–50. Thus, we can conclude that the term “security database,” as used in the ’529 Patent, encompasses *at least* a database within an inspection environment that monitors for cybersecurity threats and is configured to store a representation of a cloud computing environment that is monitored by the inspection environment. An example of such a security database is the Neo4j[®] graph database. *Id.* at 7:58–60. As discussed below, another example is the “context map” disclosed in Shua ’048. *See* Ex. 1005, 15, 25.

ii. Mapping the proposed combination to limitation 1[c]

Having reached an initial understanding of the term “security database,” we turn to Petitioner’s argument that the graph database, or “context map,” disclosed in the prior art is a “security database including a representation of the computing environment.” *See* Pet. 17–21.

Petitioner contends that “Shua describes scanning the customer’s ‘entire environment’ to ‘build a map’ of it.” Pet. 18; Ex. 1005 ¶ 33. Shua explains that “[i]n some embodiments, this map may be in a form of graph: a

plurality of interconnected vectors connecting the plurality of systems and devices, based on the networking configuration.” Ex. 1004, 13:2–5. In Shua ’048, such a map is visually represented as a graph. Pet. 18; Ex. 1005, 15; *see* Ex. 1003 ¶¶ 67–68 (attesting to authenticity of image on page 15 of Shua ’048). Petitioner further argues that “Lang teaches generating a representation of the identified [AI] model, which a POSITA would understand to have been stored with the other cloud asset representations.” Pet. 20; Ex. 1003 ¶ 105. Petitioner concludes that in the combination of Shua and Lang, Shua’s system “would capture a snapshot of a disk from a virtual machine in the customer’s cloud computing account,” and Lang’s system “would inspect files on the snapshot to identify the AI model . . . and generate an abstract representation of the AI model that can be stored in Shua’s map representing the customer’s computing environment.” Pet. 21.

Dr. Zadok summarizes Petitioner’s mapping of the prior art to limitation 1[c] as follows:

In sum, Shua in view of Lang teaches generating a representation of the AI model (adding a node in Shua’s map corresponding to the AI model detected by Lang’s analysis) in a security database (Shua’s map), the security database including a representation of the computing environment (Shua’s map including nodes representing the customer’s cloud assets, edges representing the connections between them, and attributes representing the properties of the nodes and/or connections).

Ex. 1003 ¶ 109. Thus, according to Dr. Zadok, Shua’s map is a security database.

Patent Owner argues that Petitioner has not shown that Shua discloses a representation of an AI model stored in a “security database” because “[a] map is not a database.” Prelim. Resp. 8. The ’529 Patent, however, provides that a security database may be implemented as “a graph database . . . and

the like.” Ex. 1001, 7:55–58. The evidence suggests that a graph database can be “a stored data structure representing the computing environment as nodes, edges, and attributes.” Ex. 1003 ¶ 100. Shua ’048 depicts such a graph on page 15 and labels it as a “context map.” Ex. 1005, 15 (following paragraph 36). Thus, regardless of whether all “maps” would or would not qualify as databases, the evidence indicates that the specific map depicted in Shua ’048 is a representation of a graph database. More specifically, it is a graph database that stores a representation of a cloud computing environment. *See id.*; *id.* ¶ 35 (“After a customer adds an account to Orca, the SideScanning™ process starts with building a map of the customer’s organization’s entire estate.”). Moreover, once created, this database is used within an inspection environment that monitors for cybersecurity threats. *Id.* ¶ 37 (“A categorical risk level assessment may be performed.”). The evidence currently before us suggests, therefore, that Shua’s map is an example of a “security database” as that term is used in the ’529 Patent.

Patent Owner also argues that Petitioner has not shown a motivation to combine Shua and Lang because “Petitioner’s motivation theory is self-contradicting.” Prelim. Resp. at 9–13. Petitioner asserts that a motivation would have existed because Shua expressly provides that it is desirable to scan “100% of an organization’s assets.” Pet. 11; Ex. 1005 ¶ 29; Ex. 1003 ¶ 76. Lang’s AI model would simply be stored with the other cloud asset representations shown in Shua, which emphasizes that the map should include the customer’s “entire environment.” Pet. 21; Ex. 1005 ¶ 33; Ex. 1003 ¶ 108. Patent Owner contends that by identifying AI models as cloud assets, Petitioner blurs the meaning of “assets” without explanation. Prelim. Resp. 9–10. Patent Owner argues that Shua ’048 states that virtual machines (“VMs”) are “assets,” along with other “systems and devices”

such as web servers and database servers. *Id.* at 10; Ex. 1005 ¶ 1; *see also* Ex. 1004, 13:14–25; Ex. 1003 ¶¶ 63, 102. Patent Owner then notes that according to Dr. Zadok, “an AI model would consist of code running on a VM, and captured in a snapshot.” Prelim. Resp. 11; *see* Ex. 1003 ¶¶ 89, 105–106. Patent Owner argues that it is not possible for both the VM and the AI model hosted on the VM to be “assets” as Shua ’048 uses the term. Prelim. Resp. 12 (“Petitioner’s circular logic would generate a second representation of something already included in the Shua ’048 map.”).

We find nothing contradictory in Petitioner’s argument that “100% of an organization’s assets” would include its AI models. Pet. 11, 21.

Shua ’048 appears to contemplate treating multiple layers of structures as assets to be mapped and monitored. Ex. 1005 ¶ 30 (Shua’s Orca system “automatically assesses the security state of discovered asset[s] throughout the technology stack, including all four cloud layers: I/S, OS, apps, and data.”). On the current record, a VM is an asset that contains other assets, including an AI model.¹⁰

We conclude that for the purposes of institution, Petitioner’s mapping, as elucidated by Dr. Zadok, adequately demonstrates that the combination of Shua and Lang discloses limitation 1[c] and the corresponding limitations in claims 9 and 10. We further conclude that Petitioner’s identification of a motivation to combine Shua with Lang is adequate for institution purposes.

¹⁰ This is especially so given the recognition in both Shua and Lang that the assets to be monitored include “data.” *See, e.g.*, Ex. 1004, 11:16–18 (monitoring changes in cloud environment may involve “comparing data, metadata, network connections, software configurations, firewall configurations, or any other aspects related to cloud infrastructure 106.”); Ex. 1006 ¶¶ 331–332 (analyzing containers and/or VMs for AI systems).

b. Independent Claims 1, 9, and 10: Limitation 1[e]

Patent Owner also disputes Petitioner’s arguments regarding claim limitation 1[e]. Limitation 1[e] reads “generating a representation of the cybersecurity risk in the security database, the representation of the cybersecurity risk connected to the representation of the AI model in response to detecting the cybersecurity risk[.]” Ex. 1001, 19:32–35. Petitioner argues that Shua discloses “generating a representation of the cybersecurity risk in the cybersecurity database” at least because “Shua teaches that representations of cybersecurity risks are added to its map (security database) to ‘contextualize assets and their associated risks.’” Pet. 24; Ex. 1005 ¶¶ 36, 61. Petitioner relies on an illustration in Shua ’048 demonstrating that the “context map” discussed above in connection with limitation 1[c] “has been augmented with vulnerability data.”¹¹ Pet. 25; Ex. 1005, 25 (following ¶ 64) (illustration labeled “Understanding Context”). The illustration included in the Petition, however, is a color copy of a figure in an *Orca Security SideScanning Technical Brief* that Dr. Zadok attests to be a clearer copy of the black-and-white figure provided in Shua ’048. Ex. 1003 ¶¶ 67–68; *compare* Ex. 1007, 17 *with* Ex. 1005, 25.

¹¹ To complete its mapping of the prior art to limitation 1[e], Petitioner argues that “Lang teaches generating a representation of an identified vulnerability and associating identified vulnerabilities for [an AI] model with that model” and that “a POSITA would further be motivated to add Lang’s associations of AI models with associated cybersecurity risks in Shua’s map based on Shua’s teaching that the system should ‘contextualize assets and their associated risks discovered within the customer cloud account,’ including AI assets.” Pet. 27–28; Ex. 1006, Fig. 20; Ex. 1005 ¶ 36; *see* Ex. 1003 ¶ 126. These contentions are not disputed.

Patent Owner argues that Petitioner’s analysis of limitation 1[e] is an example of Petitioner’s tendency to “rel[y] extensively on background references to fill gaps beyond what is missing in the Shua disclosures.” Prelim. Resp. 13. Patent Owner notes that for limitation 1[e], Petitioner relies on the witness testimony of Dr. Zadok, who relies on an Orca technical brief interpreted in terms of a NIST guide. *Id.*; see Ex. 1003 ¶¶ 52, 119; Ex. 1007, 17; Ex. 1016, 2. Patent Owner argues that this “meandering course” can only be explained by “impermissible hindsight, motivated by a need to address claim language[.]” Prelim. Resp. 14.

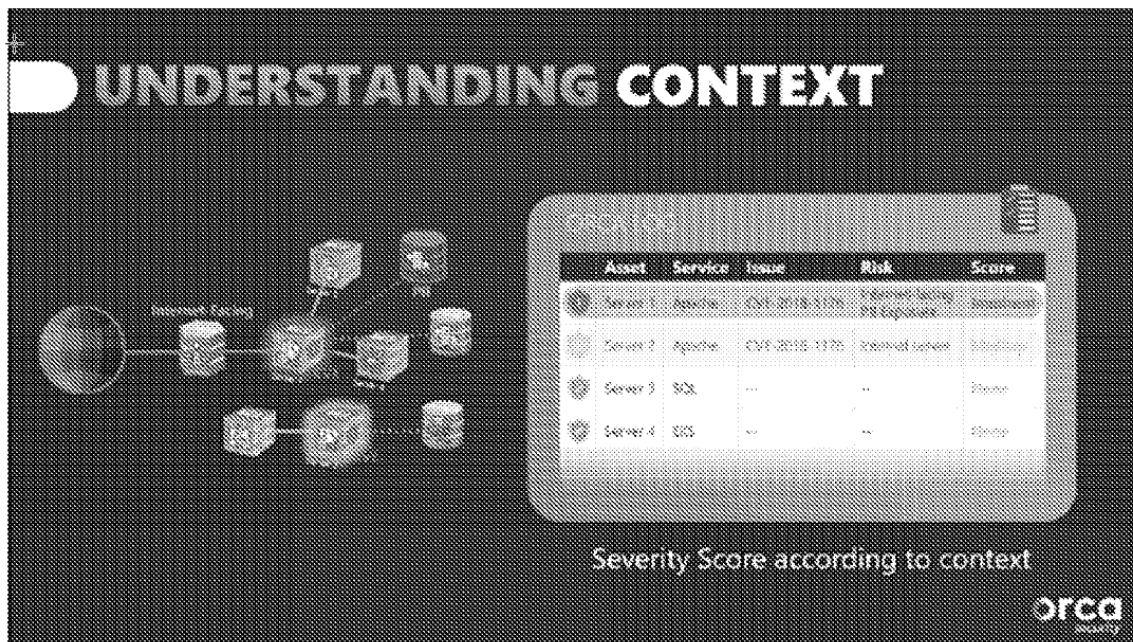
A petitioner is, of course, permitted to rely on expert testimony and references relied upon by that expert to show the knowledge of a skilled artisan. *See, e.g., Koninklijke Philips N.V. v. Google LLC*, 948 F.3d 1330, 1337–38 (Fed. Cir. 2020); *Ariosa Diagnostics v. Verinata Health, Inc.*, 805 F.3d 1359, 1365 (Fed. Cir. 2015) (“Art can legitimately serve to document the knowledge that skilled artisans would bring to bear in reading the prior art identified as producing obviousness.”). Such extrinsic evidence “may be considered when it is used to explain, but not expand, the meaning of a reference.” *In re Baxter Travenol Labs.*, 952 F.2d 388, 390 (Fed. Cir. 1991).

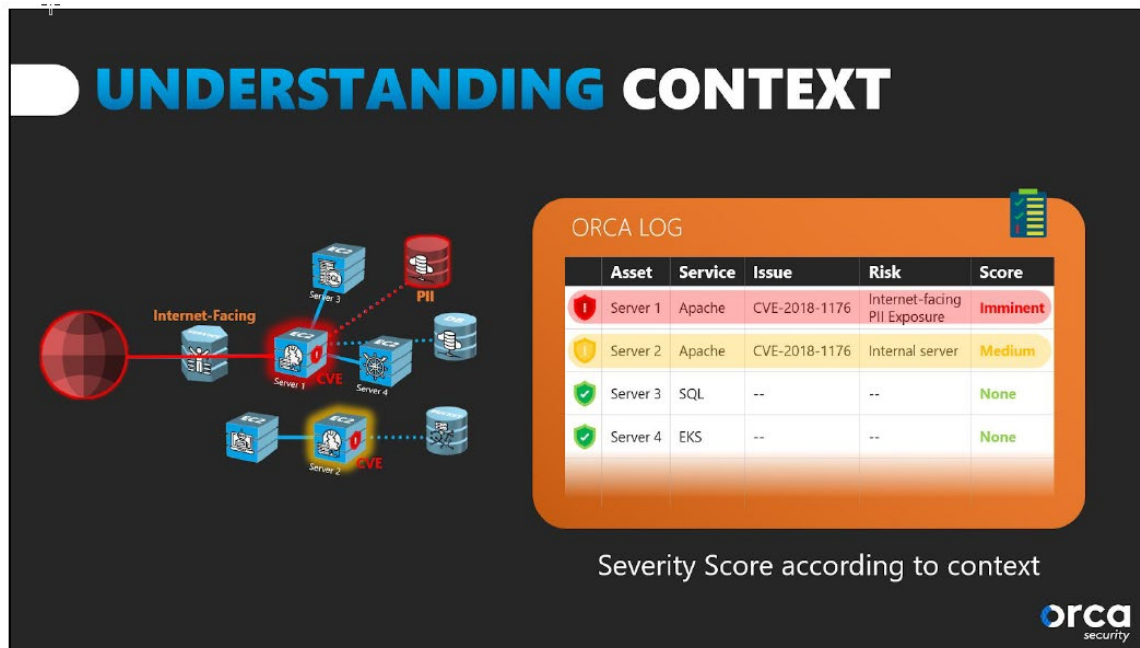
Moreover, when evaluating a combination of teachings, it is often necessary to look at, among other things, “the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.” *KSR*, 550 U.S. at 418 (citing *In re Kahn*, 441 F.3d at 988). The Federal Circuit has “emphasized the importance of a factual foundation to support a party’s claim about what one of ordinary skill in the relevant art would have known.” *Randall Mfg. v. Rea*, 733 F.3d 1355, 1362 (Fed. Cir. 2013). Thus, we understand Patent

Owner's argument to be, not that Petitioner should not have cited to background references at all, but that there is a problem with the particular sources used.

Patent Owner's principal concern appears to be with Exhibit 1007, the *Orca Security SideScanning Technical Brief*. Patent Owner argues that "[f]or element 1[e], Petitioner relies on content from EX1007 that is not found in the corresponding figure in EX1005." Prelim. Resp. 14. Patent Owner contends that Exhibit 1007, the source of the color versions of the Shua '048 figures that Petitioner relies upon as disclosing limitation 1[e], contains material that is not in Shua '048. Patent Owner argues that because Exhibit 1007 has not been shown to be prior art, it was improper for Petitioner to rely on that extraneous material.

The figures at issue in Exhibits 1005 and 1007 are reproduced below. The first figure is from Exhibit 1005, the Shua '048 provisional. The second figure is from Exhibit 1007, the source of the figure provided in the Petition.





Figures from Ex. 1005, 25; Ex. 1007, 17.

Each figure is labeled “Understanding Context.” Each depicts a map, or graph database, on the left and a table labeled “Orca Log” on the right, with a caption reading “Severity Score according to context.”

Patent Owner argues that the Petition relies on the table shown in Exhibit 1007, where “‘Server 1’ and ‘Server 2’ have been annotated with a ‘CVE’ attribute” as allegedly meeting the *representation . . . in a security database* requirement.” Prelim. Resp. 14 (quoting Pet. 25). Patent Owner contends that “none of the ‘Server 1,’ ‘Server 2,’ or ‘CVE’ text that Petitioner cites is present in the corresponding figure in EX1005.” *Id.* at 14–16 (“The content of EX1005 is not merely ‘reduced-quality’ (Pet. 18); it is indecipherable and therefore lacking the text from EX1007 that Petitioner relies on in its element 1[e] mapping.”).

While the figure in Shua ’048 is certainly a “reduced-quality” image, we disagree that it is utterly indecipherable. It is possible to read the words “Server 1,” “Server 2,” and “CVE” in the table on the right side of the

figure. More importantly, Dr. Zadok attests in his Declaration that he was able to examine and compare the two figures and that “it is [his] opinion that certain figures in *Orca Security SideScanning Technical Brief* are identical but for image quality to the corresponding figures appearing in the *Shua Provisional*.” Ex. 1003 ¶ 67. He further attests that while the higher-quality images were reproduced for the sake of readability, “it is the images from the Shua Provisional that form the basis of [his] opinions[.]” *Id.* ¶ 68.

Petitioner, in turn, relies on Dr. Zadok’s opinions as evidence of the content and meaning of Shua, including Shua ’048. *E.g.*, Pet. 25–26 (citing Ex. 1003 ¶¶ 119–122 in support of Petitioner’s 1[e] argument).

It is Dr. Zadok’s opinions in his Declaration, in addition to the image in Shua ’048, that are most relevant to Petitioner’s argument that the proposed combination discloses limitation 1[e] of the ’529 Patent. We conclude, based on the current state of the record, that that evidence, located in Exhibits 1003 and 1005, is sufficient for institution purposes to show that the cited prior art discloses limitation 1[e].

c. Dependent Claims 2–8 and 11–17

Petitioner offers an undisputed analysis applying the teachings of Shua and Lang to the additional limitations found in the challenged dependent claims. Pet. 30–46, 51–52; Ex. 1003, ¶¶ 134–180, 201–207. We find Petitioner’s analysis of the challenged dependent claims to be consistent with the evidence of record at this stage of the proceeding, including the asserted prior art and the Declaration of Erez Zadok (Ex. 1003).

3. Whether a Reasonable Expectation of Success Would Have Existed

Patent Owner’s final argument is that Petitioner has not demonstrated that one of ordinary skill in the art would have had a reasonable expectation

of success in combining the teachings of Shua '048 and Lang. Prelim. Resp. 16–17. Patent Owner argues that Petitioner “has provided no eligible basis for an obviousness determination and no reasonable expectation of success in combining the teachings of Lang (EX1006) with an IPR-eligible prior art reference.” *Id.* at 16–17. This argument is predicated on Patent Owner’s previous argument that Shua '048 is not eligible prior art, and consequently we reject the argument for the reasons discussed in Section II.E.1 above.

III. CONCLUSION

For the reasons discussed above, we determine that Petitioner has demonstrated a reasonable likelihood that it would prevail in showing that at least one claim of the '529 patent is unpatentable. Our analysis is based on the preliminary record developed thus far and may change after the record is developed fully, during trial. The parties are encouraged to address claim construction and any disputes concerning the authenticity or accuracy of submitted evidence in their briefs.

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that *inter partes* review of claims 1–17 of U.S. Patent No. 12,003,529 is *instituted* with respect to all grounds of unpatentability set forth in the Petition; and

FURTHER ORDERED that pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4(b), *inter partes* review of the '529 patent shall commence on the entry date of this Decision, and pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, notice is hereby given of the institution of a trial.

IPR2025-01087

U.S. Patent No. 12,003,529

FOR PETITIONER:

Robin A. Snader

Eric A. Buresh

Christopher R. Schmidt

Kathleen Fitterling

ERISE IP, P.A.

robin.snader@eriseip.com

eric.buresh@eriseip.com

kathleen.fitterling@eriseip.com

chris.schmidt@eriseip.com

FOR PATENT OWNER:

Matthew A. Argenti

Michael T. Rosato

Wesley E. Derryberry

Joseph M. Baillargeon

WILSON SONSINI GOODRICH & ROSATI

margenti@wsgr.com

mrosato@wsgr.com

wderryberry@wsgr.com

jbaillargeon@wsgr.com