

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner,

v.

K.MIZRA LLC,
Patent Owner.

Case IPR2025-01436
Patent 8,234,705

PATENT OWNER'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

I. INTRODUCTION1

II. THE ’705 PATENT2

III. CLAIM CONSTRUCTION6

IV. ANALYSIS.....7

 A. Petitioner Fails to Establish That Element [1.5] is Satisfied in
 its Asserted Combination of References8

 B. Petitioner Fails to Establish How Claim 1 is Obvious Over
 Freund, Ball, Pujare *and* Lewis14

 C. Petitioner’s Competing and Contradictory Claim Construction
 Positions Also Require Denial17

 D. Independent Claims 12 and 19 and the Dependent Claims are
 also Patentable Over Petitioner’s Challenge for the Same
 Reasons Stated Above20

 E. Petitioner’s Motivation to Combine the Asserted References
 Suffers from Hindsight Reconstruction Bias20

 i. The Combination of References for Element [1.2] is
 Unsupported21

 ii. The Combination of References for Element [1.9] Destroys
 an Advantage of Freund23

V. CONCLUSION.....25

TABLE OF AUTHORITIES

Cases

Canon Inc. v. WSOU Investment, LLC,
IPR2022-01532, Paper 14 (PTAB Apr. 14, 2023)15

Cuzzo Speed Techs., LLC v. Lee,
579 U.S. 261 (2016).....17

EIK Eng’g SDN. BHD. v. Wilco Marsh Buggies & Draglines, Inc.,
IPR2020-00344, Paper 12 (PTAB Mar. 4, 2021)14

EIK Eng’g SDN. BHD. v. Wilco Marsh Buggies & Draglines, Inc.,
IPR2020-00344, Paper 7 (PTAB June 23, 2020)14

Intuitive Surgical, Inc. v. Ethicon LLC,
25 F.4th 1035 (Fed. Cir. 2022)14

MIM Software Inc. v. Progenics Pharms., Inc.,
IPR2025-00725, Paper 13 (PTAB Oct. 8, 2025)20

SuperGuide Corp. v. DirecTV Enters., Inc.,
358 F.3d 870 (Fed. Cir. 2004)6

Statutes

35 U.S.C. § 312(a)(3)..... 15, 18, 19

Rules

37 C.F.R. § 42.10415

37 C.F.R. § 42.1071

37 C.F.R. § 42.619

PATENT OWNER’S EXHIBIT LIST

Exhibit No.	Description
2001	Complaint for Declaratory Judgment of Non-Infringement of U.S. Patent Nos. 8,144,717 and 8,438,120, <i>Google LLC v. K.Mizra LLC</i> , No. 3:25-cv-08107-JCS (N.D. Cal.) (ECF No. 1)
2002	U.S. Patent No. 9,420,065 to Mayo et al.
2003	Screenshot of web page “Cisco Systems Inc. Be The Bridge to Possible” (https://www.cloud.google.com/find-apartner/partner/cisco-systems-inc , last accessed Nov. 21, 2025) and “Cisco and Googler partner on a new open hybrid cloud solution spanning on-premises environments and Google Cloud Platform” (https://www.cloud.google.com/find-apartner/partner/cisco-systems-inc , last accessed Nov. 21, 2025)
2004	Screenshot of web page “Hewlett Packard Enterprise Delivering true hybrid cloud for containers” (https://cloud.google.com/find-apartner/partner/cloud-technology-partners-ctp-an-hpe-company , last accessed Nov. 21, 2025) and “Enterprise partner to deliver hybrid cloud solutions to customers” (https://cloud.google.com/blog/topics/partners/google-cloudpartners-with-hpe-on-hybrid-cloud-next19 , last accessed Nov. 21, 2025)
2005	Declaration of Charles J. Hausman in Support of Patent Owner’s Request for Discretionary Denial
2006	Patent and Trademark Office, Notice of Proposed Rulemaking - Revision to Rules of Practice before the Patent Trial and Appeal Board, https://federalregister.gov/d/2025-19580 , Oct. 17, 2025
2007	Scheduling Order, <i>K.Mizra LLC v. Google LLC</i> , 1:25-cv-00236-ADA (W.D. Tex.) (ECF No. 39)
2008	Standing Order Governing Proceedings (OGP) – Patent Cases, J. Albright (W.D. Tex.)
2009	Screenshot of Trial Statistics 01/01/2009 – 10/16/2025, U.S. District Court for the Western District of Texas
2010	Order Denying Motion to Dismiss, <i>K.Mizra LLC v. Google LLC</i> , 1:25-cv-00236-ADA (W.D. Tex., Oct. 22, 2025)

IPR2025-01436 Patent Owner’s Preliminary Response

2011	Claim Construction Order and Memorandum in Support Thereof, <i>K.Mizra LLC v. Google LLC</i> , 1:25-cv-00236-ADA (W.D. Tex.) (ECF No. 57)
2012	Order Setting Trial Date & Discovery Deadlines, Referring Case to Mediation & Referring Discovery Motions to United States Magistrate Judge, <i>K.Mizra LLC v. Citrix Systems, Inc. et al.</i> , No. 0:25-cv-60803-WPD (S.D. Fla.) (ECF No. 46)
2013	Screenshot of Judge William P. Dimitrouleas Median Time-to-Trial Statistics, U.S. District Court for the Southern District of Florida
2014	Clerk’s Notice of Judge Assignment to Judge William P. Dimitrouleas, <i>K.Mizra LLC v. Citrix Systems, Inc. et al.</i> , No. 0:25-cv-60803-WPD (S.D. Fla.) (ECF No. 20)
2015	Order Denying Defendant’s Motion to Dismiss, <i>K.Mizra LLC v. Citrix Systems, Inc. et al.</i> , No. 0:25-cv-60803-WPD (S.D. Fla.) (ECF No. 34)
2016	Google, LLC’s Invalidity Contentions, <i>K.Mizra LLC v. Google LLC</i> , 1:25-cv-00236-ADA (W.D. Tex.) (July 15, 2025)
2017	Defendants’ Amended Answer and Affirmative Defenses to Plaintiff’s Complaint, <i>K.Mizra LLC v. Citrix Systems, Inc. et al.</i> , No. 0:25-cv-60803-WPD (S.D. Fla.) (ECF No. 44)
2018	Patent and Trademark Office, Interim Director Discretionary Process, https://www.uspto.gov/patents/ptab/interim-directordiscretionary-process , Nov. 21, 2025
2019	Complaint for Patent Infringement, <i>K.Mizra LLC v. Google LLC</i> , 1:25-cv-00236-ADA (W.D. Tex.) (ECF No. 1)

IPR2025-01436 Patent Owner’s Preliminary Response

Pursuant to 37 C.F.R. § 42.107, Patent Owner K.Mizra LLC (“K.Mizra” or “Patent Owner”) files this preliminary response to the Petition, setting forth reasons why the Petition for *inter partes* review (“IPR”) of claims 1-19 of U.S. Patent No. 8,234,705 (the “’705 patent”), as requested by Google LLC (“Petitioner”), should be denied on the merits.

I. INTRODUCTION

The ’705 patent, which has a priority date going back to September 27, 2004, claims a technique to control access to secure computer networks by detecting the health and compliance status of a computer in a trusted manner and allowing remediation of the computer to ensure compliance with network security policies. See, e.g., Ex. 1001, Abst. The ’705 patent’s solution verifies that any device attempting to access a company’s network meets standards for network security and will not introduce dangerous computer programs or viruses into the network. A novel aspect of the invention lies in this verification—an attestation of cleanliness transmitted from a trusted computing base associated with a trusted platform module. The inventors of the ’705 patent recognized the potential risk of false attestations as a further significant security hole. Accordingly, they believed sending a secure message with an attestation from a trusted computing base associated with a tamper-resistant trusted platform module in a host to be a significant point of innovation.

The Petition challenges the claims of the '705 patent based on the proposed combination of Freund (Ex. 1005), Ball (Ex. 1006), Pujare (Ex. 1009), and Lewis (Ex. 1013). However, this combination is unsupported by credible and supportable motivation to combine these references, and instead the Petition relies on hindsight-based reasoning to recreate the challenged claims. Additionally, Petitioner interprets the “at least one of ... and” portion of element [1.5] in the conjunctive, but fails to establish every claimed feature in its asserted combination. Thus, not only is the combination unsupported by proper motivation, but the asserted combination fails to disclose element [1.5] according to Petitioner's asserted construction. No IPR should be instituted.

II. THE '705 PATENT

The '705 patent is titled “Contagion Isolation and Inoculation” and was issued by the United States Patent Office to inventors James A. Roskind and Aaron R. Emigh on July 31, 2012. The earliest application related to the '705 patent was filed on September 27, 2004. *See* '705 patent, cover.

The '705 patent is directed to methods and systems for securing a computer network by detecting viruses and/or vulnerabilities on a computer attempting to access a secure network, quarantining the computer by restricting access to the network upon detection of an infestation or vulnerability, and permitting limited

access to the protected network for remedying the insecure condition on the computer. '705 patent, Abst., 11:15-12:13.

Prior art computer network security systems faced considerable challenges with protecting and maintaining up-to-date security software on mobile devices such as employees' personal laptops, which posed significant security risks that could allow attackers or viruses stealth access into a business's network, bypassing IT security measures. *Id.*, 1:34-38. While a network security appliance or hardware can adeptly keep out unwanted external intrusions into the network, the most exploitable vulnerabilities of a computer network are found on the end-user computers that roam throughout various other insecure public and private network domains and then access the presumably secure network day in and day out. *Id.*

The '705 patent closes this loophole by verifying that any device attempting to access a company's network meets its standards for network security and will not introduce dangerous computer programs or viruses into the network. As noted in the introduction, a novel aspect of the invention lies in this verification—a signed attestation of cleanliness from a trusted computing base associated with a trusted platform module. *See, e.g.*, '705 patent, at Claim 1, 13:64-14:12; Ex. 1002, 185 (Jan. 10, 2010 Office Action Response at p. 8). The inventors of the '705 patent recognized the potential risk of false attestations as a further significant security hole. Accordingly, they believed providing a securely-signed attestation

from a trusted computing base associated with a tamper-resistant trusted platform module to be a significant point of innovation. *See, e.g.*, Ex. 1002, 185 (Jan. 10, 2010 Office Action Response at p. 8).

Furthermore, when “a request is received from a host, e.g., via a network interface, to connect to a protected network, it is determined whether the host is required to be quarantined. If the host is required to be quarantined, the host is provided . . . limited access to the protected network . . . only as required to remedy a condition that caused the quarantine to be imposed, such as to download a software patch, update, or definition; install, remove, and/or configure software and/or settings as required by a policy; and/or to have a scan or other diagnostic and/or remedial operation performed.” ’705 patent, 3:8-20.

Relevant to these disclosures, challenged claim 1 recites (with emphasis added):

1. A method for protecting a network, comprising:
detecting an insecure condition on a first host that has
connected or is attempting to connect to a
protected network, wherein detecting the insecure
condition includes *contacting a trusted computing
base associated with a trusted platform module
within the first host*, receiving a response, and
determining whether the response includes a valid
digitally signed attestation of cleanliness, *wherein*

the valid digitally signed attestation of cleanliness includes at least one of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host;

when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network, wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes receiving a service request sent by the first host, serving a quarantine notification page to the first host when the service request comprises a web server request, and *in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page* if a host name that is the subject of the DNS query is not associated with a remediation host configured to provide data usable to remedy the insecure condition; and permitting the first host to communicate with the remediation host.

While only claim 1 has been reproduced here, independent claims 12 and 19 include substantially similar limitations as those emphasized above, and are patentable over Petitioner’s challenge for the same reasons presented in this POPR for claim 1.

III. CLAIM CONSTRUCTION

Petitioner presents the proposed and agreed-upon constructions for eight terms identified in the “Related Litigation.”¹ Of relevance to the merits defects addressed below, Petitioner notes that the parties have agreed that the claimed “trusted platform module” should be construed as “a secure cryptoprocessor that can store cryptographic keys and that implements the Trusted Platform Module specification from the Trusted Computing Group.” Pet., 17.

Petitioner also submits to the District Court that “includes at least one of an . . . and an . . .” should be construed in the conjunctive, thus meaning “includes at least one of an . . . and at least one of an . . .” Pet., 17; Ex. 1014, 11-13 (applying *SuperGuide Corp. v. DirecTV Enters., Inc.*, 358 F.3d 870, 886 (Fed. Cir. 2004)). As will be discussed below, Petitioner attempts to show that its asserted art discloses or suggests the conjunctive form of this claimed feature. But Petitioner’s

¹ *K.Mizra LLC v. Google LLC*, Civ. Action No. 1:25- cv-00236 (W.D. Tex.). See Ex. 1014, Ex. 1015; see also Pet., 16-20.

hand-waving theory comes up short as to this term, and the challenge therefore fails on the merits.

IV. ANALYSIS

Petitioner’s challenges are based on a combination of Freund, Ball, Pujare, and Lewis references.² However, Petitioner’s alleged motivation to combine these references is tainted by impermissible hindsight. Further, even if combined, the combination fails to disclose every claimed feature according to Petitioner’s alleged constructions. Namely, Petitioner asserts to the District Court that element [1.5] requires that “valid digitally signed attestation of cleanliness” sent from the trusted computing base must include both “an attestation that the trusted computing base has ascertained that the first host is not infested,” *and also* “an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host.” Pet., 18; Ex. 1014, 11-13

² See Pet., 8:

Ground	Reference(s)	Basis	Claims
1	U.S. Patent Application Publication No. 2003/0055962 to G. Freund <i>et al.</i> (“Freund”) (EX1005) in view of U.S. Patent Application Publication No. 2006/0005009 to C. Ball <i>et al.</i> (“Ball”) (EX1006), U.S. Patent Application Publication No. 2002/0083183 to Pujare <i>et al.</i> (“Pujare”) (EX1009), and U.S. Patent No. 7,533,407 to Lewis <i>et al.</i> (“Lewis”) (EX1013)	103	1-19

(arguing that *SuperGuide* controls this construction). The Petition fails to establish both of these elements in the asserted challenge.

A. Petitioner Fails to Establish That Element [1.5] is Satisfied in its Asserted Combination of References

As noted above, claim 1 of the '705 patent recites a “method for protecting a network,” where the first element recites, in relevant part, “detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network, wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host, receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness, *wherein the valid digitally signed attestation of cleanliness includes at least one of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host ...*.” Claim 1 (emphasis added). According to Petitioner's claim construction position, the claimed “valid digitally signed attestation of cleanliness” sent from the trusted computing base must include both “an attestation that the trusted computing base has ascertained that the first host is not infested,” *and also* “an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host.” Pet., 18;

Ex. 1014, 11-13 (arguing that *SuperGuide* controls this construction). Under this interpretation of element [1.5], Petitioner’s challenge fails because Petitioner fails to establish that both required elements are contained in a response from Freund’s computer to the router-side CMP.

In addressing element [1.5], the Petition relies on Freund alone for this claimed feature. Pet., 31-34. To address the second requirement, Petitioner specifically asserts that Freund “receives an attestation of the presence of an anti-virus version update - i.e., patch or a patch level associated with a software component of the first host.” Pet., 31. But to address the first requirement—an attestation that the trusted computing base has ascertained that the first host is not infested—Petitioner asserts that Freund’s “router CMP challenge verifies that the first host is running an antivirus program.” *Id.* This assertion falls short and renders Petitioner’s challenge meritless. The overarching defect in the Petition is that Petitioner fails to advance a disclosure-based theory of how Freund allegedly discloses “an attestation that the trusted computing base has ascertained that the first host is not infested” and includes that attestation in the response to the router.

Petitioner generally asserts that “Freund’s valid digitally signed attestation of cleanliness attests that the first host is not infested by attesting that the anti-virus software is running and/or that anti-virus real-time monitoring is enabled.” Pet., 32. The cited support for Petitioner’s assertion is Freund, [0110]-[0117]. Pet., 32.

But these paragraphs do not support Petitioner’s interpretation of Freund. Instead, these paragraphs are directed to computers that are out-of-compliance and require corrections. For example, Freund discloses that the sandbox server includes various ports that may receive redirected communications identifying errors in the client computer. Freund discloses those ports and errors in [0117], reproduced below:

Port	Content
80	General help and trouble shooting.
8080	Redirect Base Port.
8081	Client Time Out.
8082	No client response.
8083–8112	Reserved
8113	Wrong client version. Prompts user to update ZAP with new version.
8114	Invalid license key. Informs user their license key is invalid-contact administrator.
8115	Informs user that the ZAP license is insufficient for number of users-contact administrator.
8116	Anti-virus not installed. Informs user that he/she needs to download anti-virus software.
8117	Anti-virus old. Informs user to update anti-virus software.
8118	Anti-virus auto-update not enabled. Informs user to activate anti-virus Auto-Update.
8119	Anti-virus Real-Time monitoring not enabled. Informs user to activate Real-Time monitoring.

But these are all error codes indicating that there is *no* attestation of cleanliness. What Petitioner fails to do throughout the Petition is address what is transmitted in Freund that satisfies “an attestation that *the trusted computing base has ascertained that the first host is not infested,*” as claimed. (emphasis added). Even Freund’s client response interpretation disclosure addresses values associated with defects rather than identifying the content of an attestation of cleanliness. Freund’s client response interpretation values are disclosed in [0144], reproduced below.

IPR2025-01436 Patent Owner’s Preliminary Response

Response	Value	Comment
Client time out	1	No recent valid client response.
No client response	2	No client response ever received.
Reserved	3–32	Reserved.
ZAP version outdated	33	Client application incorrect or old.
Invalid license	34	Invalid license key, contact administrator.
License exceeded	35	Max users exceeded for license - contact administrator.
No Antivirus program installed	36	AV not installed.
Antivirus wrong version	37	AVold version.
Antivirus Auto-Update not configured	38	AV Auto-Update is not configured.
Antivirus Real-Time Monitor not running	39	AV Real-Time Monitor not running on client
Packet time stamp	>256	Current time stamp in seconds + 256

As can be seen here in the client response table, these values and comments all correspond to a computer that is *out of compliance* or a timestamp that the router can use to make its own determination of cleanliness. *See* Freund, [0088], [0149].

Petitioner also asserts that “Freund’s attestation of cleanliness confirms that anti-virus software is updated with any recent updates represented by patch or patch level updates to the anti-virus software.” Pet., 33 (citing Freund, [0078], [0085]). But these paragraphs fall short in supporting that a client transmits an attestation of cleanliness. Once again, Freund’s [0078] is focused on non-compliant computers, and fails to disclose any alleged “attestation of cleanliness” from the host to the router-side CMP.

Petitioner’s reliance on Freund’s [0085] also falls short. While Petitioner cites to [0085] in its Petition for element [1.5] (*see* Pet., 31, 33), Petitioner fails to analyze [0085]’s disclosures as they bear on element [1.5]. Per [0085], Freund

discloses that “the router-side CMP component may also (optionally) enforce other security policies in addition to requiring the local computers to be running the specified end point security module” and the “CMP would then evaluate whether or not each local computer was in compliance with the specified policy.” Freund, [0085]. The problem here is that Petitioner requires the client to respond with a “valid digitally signed attestation of cleanliness [that] includes at least one of an attestation that the trusted computing base has ascertained that the first host is not infested,” but Petitioner then cites to a paragraph of Freund that requires the router-side CMP, not the client computer, to make a determination of whether the client computer (or host) is in compliance with a policy. Petitioner makes no effort to reconcile these seemingly-conflicting positions.

Petitioner tries to brush over its lack of analysis in this regard by asserting that the “’705 Patent discloses that a first host is ‘not infested’” via certain disclosures. Pet., 32. What Petitioner overlooks is the specification of the ’705 patent teaches more than Petitioner recognizes. For example, the ’705 patent explains that “a *sufficiently updated* software and/or scan may act as a cleanliness assertion.” ’705 patent, 14:15-19 (emphasis added). Freund instead is focused on the ways in which a client computer is *out of compliance*. For example, from Freund’s port listings in [0117] reproduced above, a client computer could have real-time monitoring enabled, but the anti-virus software could be old (port 8117)

or the anti-virus auto-update might not be enabled (port 8118). Once again, Petitioner fails to address what an “attestation of cleanliness” looks like in Freund, and instead discusses and cites over and over to Freund’s paragraphs disclosing non-compliant computers. *See* Pet., 33-34 (discussing quarantine procedures in Freund when a computer is not trusted, and how to handle responses from a computer running an “older version” of the security software).

Thus, Petitioner’s assertion that Freund’s response satisfies the claimed requirements in the ’705 patent claims is conclusory and lacks support. Despite pointing to no disclosure in Freund that allegedly discloses “an attestation that the TCB has ascertained that the first host is not infested,” Petitioner asserts the contrary without support. *See* Pet., 34.

Thus, even if Petitioner has established a valid motivation to combine the asserted reference (which Patent Owner disputes and will address in more detail below), Petitioner’s theory of unpatentability fails to consider or reconcile the actual disclosures of Freund and how those disclosures support every claimed feature in the challenged claims. The Petition suffers from overwhelming failures of proof on the merits and should be denied.

B. Petitioner Fails to Establish How Claim 1 is Obvious Over Freund, Ball, Pujare *and* Lewis

Petitioner has also failed to support its challenge because it does not explain how the asserted combination of Freund, Ball, Pujare, *and* Lewis renders the claim obvious.

The Federal Circuit has often noted that the party seeking institution of *inter partes* review is “the master of its own petition.” *See Intuitive Surgical, Inc. v. Ethicon LLC*, 25 F.4th 1035, 1041 (Fed. Cir. 2022). The Board has accordingly recognized that the “focus” of its analysis is “on what is asserted in the Petition.” *EIK Eng’g SDN. BHD. v. Wilco Marsh Buggies & Draglines, Inc.*, IPR2020-00344, Paper 7, 7 (PTAB June 23, 2020).

Here, Petitioner asserts a single ground based on Freund in view of Ball, Pujare, and Lewis. Pet., 8. Petitioner’s expert adopted this same ground. *See* Ex. 1010, ¶26. To support this ground, Petitioner was required to “identify with particularity what disclosure is relied on from each of the references[], how it would be combined with the other disclosures, and why the proposed combination would have been obvious to a person of ordinary skill in the relevant technology.” *EIK Eng’g*, IPR2020-00344, Paper 7, 14; *see also id.*, Paper 12, 9-10 (PTAB Mar. 4, 2021) (noting Petitioner needs to explain what each of the identified references contributed to the asserted unpatentability and “why it would have been obvious to combine selected disclosures from each of the three references.”).

IPR2025-01436 Patent Owner's Preliminary Response

In at least two respects, Petitioner has failed to satisfy the statutory requirements for its Petition. *See* 35 U.S.C. § 312(a)(3) (requiring Petitioner to identify “with particularity . . . the grounds on which the challenge to each claim is based, and the evidence that supports the grounds for the challenge to each claim.”); *see also* 37 C.F.R. §§ 42.104(b)(3)-(5).

Petitioner completely fails to identify how Pujare allegedly discloses or suggests any element of the challenged claims, or how or why a POSITA would be motivated to combine Pujare with Freund, Ball, and Lewis. Indeed, except in the heading, Pujare is not mentioned by name at all in the section of the Petition that “detail[s] how Claims 1-19 are [allegedly] obvious over the prior art.” *See* Pet., 20. And the exhibit is cited only once without any explanation of its relevance to the challenge. *Id.*, 34. The Petition also does not address any motivation to combine Pujare with Freund, Ball, and/or Lewis.

A similar situation was presented in *Canon Inc. v. WSOU Investment, LLC*, IPR2022-01532. In that proceeding, the Petitioner challenged claims as obvious over Sugitani and Kubo. *Id.*, Paper 14, 6 (PTAB Apr. 14, 2023). The Board found that the Petitioner had failed to establish a motivation to combine these references. *Id.*, 20. The Board acknowledged that for certain claims, the Petition “rel[ie]d on Kubo sparingly, if at all.” *Id.*, 20 n.8. However, the Board found that it “cannot deviate from the grounds in the petition and raise our own obviousness theory, e.g.,

obviousness based on Sugitani alone.” *Id.* The Board therefore concluded that “even where Kubo might not be necessary for teaching the limitations of certain claims, we evaluate Petitioner’s obviousness ground as it has been presented in the Petition, which necessarily includes Petitioner’s rationale for combining Kubo with Sugitani.” *Id.* Here, too, the Board should honor Petitioner’s decision not to raise any obviousness theory based on Freund, Ball, and Lewis alone.

Petitioner’s disclosure with respect to Lewis also fails. Although Lewis, too, is identified as a part of the combination forming the grounds for invalidity alleged in the Petition, the details here are likewise unclear. With respect to claim 1, Lewis is cited only in connection with element [1.9]. *See* Pet., 41-42. However, Petitioner argues that “Freund satisfies limitation [1.9],” implying that Lewis may not be part of the grounds at all. *Id.*, 41. Indeed, Petitioner elsewhere describes Lewis as an “alternative technique to the technique disclosed by Freund” and as providing “backup support for Freund’s disclosure of a particular claimed feature.” *Id.*, 15. And Petitioner further suggests that Lewis may only be relevant “should it be argued that the claim is somehow limited to the non-limiting exemplary embodiments disclosed in the ‘705 specification.” *Id.*, 41. It thus appears that Petitioner’s single ground may in fact be two separate grounds: a first ground based on Freund, Ball, and Pujare, and a second ground based on Freund, Ball, Pujare, and Lewis that is only relevant if the claim is limited to exemplary

embodiments in the patent specification (an argument that Petitioner, despite its various proposed constructions, has not in fact made). Neither Patent Owner nor the Board should be required to parse the Petition to figure out what the challenge actually being presented is.

Petitioner chose to allege obviousness based on Freund, Ball, Pujare, and Lewis, and has failed to properly support that challenge. The Board should limit Petitioner to its theories and not adopt its own obviousness theory based on Freund and Ball alone. As Justice Alito has explained, “if the Patent Office institutes review on claims or grounds not raised in the petition[,] the patent owner is forced to shoot into the dark” when it files its response. *Cuzzo Speed Techs., LLC v. Lee*, 579 U.S. 261, 296 (2016) (Alito, J., concurring in part and dissenting in part). “The potential for unfairness is obvious.” *Id.*

C. Petitioner's Competing and Contradictory Claim Construction Positions Also Require Denial

Petitioner also chose to offer competing claim constructions rather than selecting one. Pet., 16-20. This choice not only presents unnecessary issues for the Board, but also resulted in Petitioner being unable to properly address the claims under the appropriate claim construction.

The competing claim constructions required Petitioner to adopt confusing and contradictory interpretations of what element of the prior art meets the claim limitations. For example, Petitioner proposes competing constructions of “trusted

computing base” (“TCB”) that disagree about whether the TCB must be within the first host. Pet., 17. This forces Petitioner to take the position that “Freund’s router-side CMP and/or client-side security module satisfy the claimed TCB.” Pet., 24. But because the CMP appears to be on the “router-side” rather than within the alleged first host, this leaves it completely unclear how Petitioner alleges the limitation is met. Is it Petitioner’s contention that only a part of the TCB has to be within the first host under its construction? If not, is it Petitioner’s contention that the CMP may or may not be a part of the TCB (and, if so, how should the Board make that decision)? Neither Patent Owner nor the Board should be required to guess how Petitioner believes the claim is invalid under the proposed constructions. At the very least, Petitioner fails to describe evidence supporting its grounds “with particularity” as required by 35 U.S.C. § 312(a)(3).

The competing claim constructions also resulted in Petitioner failing to properly develop its obviousness arguments for some limitations. For example, Petitioner improperly alleged that “remediation host” is a mean-plus-function term and thus indefinite. Pet., 18. Petitioner also identified, without explanation, certain corresponding structure. Pet., 18-19. But Petitioner fails to develop any argument about how the prior art allegedly discloses the corresponding structure. Instead, the entirety of Petitioner’s argument about how the ‘705 Patent is

allegedly invalid under its proposed “means plus function” construction is two sentences:

To the extent this limitation is interpreted under §112(f)/¶6, Freund discloses corresponding structure at least to the same extent as the '705 Patent. Freund discloses a quarantine server and remediation host under any construction. *See* EX1014, pp.2-3. EX1010, ¶203.

Pet., 44. The first sentence is a conclusion that does not explain what in Freund is this “corresponding structure” or where it might be found. And the citations to the second sentence include a citation to a paragraph in the expert declaration that simply parrots the paragraph in the Petition without further explanation.

203. To the extent this limitation is interpreted under §112(f)/¶6, Freund discloses corresponding structure at least to the same extent as the '705 Patent. Freund discloses a quarantine server and remediation host under any construction. *See* EX1014

Ex. 1010, ¶203. The other citation is to Petitioner's claim construction brief from district court that addresses the “protected network” term. But even if the cited pages were relevant, this argument simultaneously violates both 35 U.S.C. § 312(a)(3) (requiring Petitioner to explain its grounds “with particularity”) and 37 C.F.R. § 42.6(a)(3) (prohibiting incorporation by reference). Nowhere does

Petitioner explain how the “corresponding structure” in Freund, whatever it may be, is equivalent to the structure described in Petitioner’s proposed construction.

Even if Petitioner’s approach of offering competing potential constructions were appropriate, it would still be Petitioner’s burden to support its challenges under the proposed constructions. *See, e.g., MIM Software Inc. v. Progenics Pharms., Inc.*, IPR2025-00725, Paper 13, 7 (PTAB Oct. 8, 2025) (noting that a petition must include “an explanation of how the prior art renders the claims unpatentable under alternative constructions”). Petitioner has failed to do so, and the Petition should therefore be denied.

D. Independent Claims 12 and 19 and the Dependent Claims are also Patentable Over Petitioner’s Challenge for the Same Reasons Stated Above

Claims 12 and 19 contain similar limitations as claim 1 and therefore survive Petitioner’s unsupported challenges for the same reasons presented above. Additionally, dependent claims 2-11 depend from independent claim 1, and dependent claims 13-18 depend from independent claim 12. For the same reasons set forth for independent claim 1 above, all of the remaining challenged claims are also patentable over the combination of Freund, Ball, Pujare, and Lewis.

E. Petitioner’s Motivation to Combine the Asserted References Suffers from Hindsight Reconstruction Bias

Finally, Petitioner’s combination of references is clearly guided by impermissible hindsight and fails.

i. The Combination of References for Element [1.2] is Unsupported

Element [1.2] requires in part “a trusted computing base associated with a trusted platform module within the first host.” According to Petitioner, Freund contacts a “trusted computing base (TCB) configured as Freund’s ‘client monitoring protocol software’ (CMP) and/or ‘client-side security component/module’ associated with a TPM within the first host.” Pet., 24. Petitioner goes on to describe the operation of Freund’s client-side security module, including the use of digital signatures, to conclude that “Freund’s disclosure of the client-side security module constitutes a TCB given that the client-side security module is hardware and/or software within the first host that provides security to the host.” Pet., 25.

Petitioner next concedes that Freund fails to disclose that Freund’s client-side security module is a “trusted platform module” as required by the claim, and argues that “a substitution of known TPM hardware to implement enhanced functionality of Freund’s TCB would have achieved predictable results with a reasonable expectation of success” Pet., 26. But Petitioner offers no advantage or improvement that would be achieved through this substitution, and no credible motivation to much such a change.

Rather, Petitioner’s litany of alleged reasons to replace Freund’s TCB with a TPM “based on Ball’s teachings” reads like a list of features that Freund’s TCB

already achieves. For example, Petitioner alleges that this substitution “would have allowed Freund’s client-side host to verify its trustworthiness by securely communicating accurate information regarding antivirus versions, anti-virus status, security compliance, and digitally signed applications using cryptographic data keys to generate digital signatures and encryption/decryption.” Pet., 26-27. But these are all features that Petitioner alleged were already present in Freund’s TCB. Aside from the clear attempt to recreate the challenged claim, Petitioner offers no reason why a POSITA would have been motivated to make this proposed swap-out of Freund’s client-side security module for Ball’s TPM.

At best, Petitioner contends that Ball’s TPM would have provided “enhanced” security and trust, but Petitioner fails to explain why that it is, or what would be allegedly “enhanced” relative to what Freund already achieves. *See* Pet., 27 (alleging that “Ball’s TPM would have provided enhanced hardware-based security,” “enhanced trust in the security configuration of Freund’s client-side device,” and “enhanced hardware-based security features.”). Undercutting any claim that Ball’s TPM would have been an improvement to Freund, Petitioner concedes that “Ball and Freund disclose similar goals of enhanced trust and security and similar mechanisms of a challenge/response protocol to determine the trustworthiness of a device.” Pet., 27.

Finally, confirming Petitioner's shotgun approach to this motivation analysis, Petitioner concludes that "it would have been *obvious to try* the TPM from among the finite number of identified, predictable hardware solutions for executing software security modules of the type disclosed by Freund with a reasonable expectation of success." Pet., 28-29. Of course the Petition makes no effort to enumerate these alleged "finite number of identified, predictable hardware solutions," thus reinforcing that Petitioner is just regurgitating pejorative obviousness theories in an effort to brush past the lack of meaningful analysis.

For all these reasons, Petitioner's proposal to modify Freund in view of Ball in an effort to satisfy element [1.2] is unsupported and fails.

ii. The Combination of References for Element [1.9] Destroys an Advantage of Freund

Element [1.9] requires in part "in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host configured to provide data usable to remedy the insecure condition." In attempting to satisfy this claimed element, Petitioner proposes to modify Freund's technique for handling a "non-compliant device" DNS query in view of Lewis. Pet., 41-42. Petitioner specifically argues that "It would have been obvious to provide the IP address of Freund's sandbox quarantine server in response to Freund's DNS query by a DNS

server as disclosed by Lewis, rather than at a router as disclosed by Freund.” Pet., 41.

But Petitioner overlooks that Freund does more than replace a destination IP address for a non-compliant device with the IP address of the sandbox server. *See* Freund, [0149]. Freund also sets the destination port in the HTTP header to match the non-compliant device's value in the router compliance table plus 8080. *Id.* This process “conveys information to the sandbox server in the HTTP header permitting the sandbox server to categorize the reason for non-compliance” and allows the sandbox server to display “a page with information enabling the client to address the specific problem that was detected.” *Id.* This process is predicated on a DNS query passing through and returning a non-exempt destination address. If the DNS replacement used in Lewis were present in Freund, no HTTP request following a DNS query would ever reach Freund's HTTP redirection (step 950) because the DNS query would return the exempt IP address of the sandbox server (step 920), which would then be used to formulate the HTTP request.

Thus, Petitioner fails to consider how Freund's process provides this advantage, and also fails to consider that the proposed modification of Freund in view of Lewis destroys this advantage. Contrary to Petitioner's assertion, a POSITA faced with Freund and Lewis would not have eliminated this advantage of Freund.

V. CONCLUSION

For the reasons presented above, Patent Owner respectfully asks that the Director deny the Petition on the merits. No *inter partes* review should be instituted.

Dated: December 23, 2025

/Wayne M. Helge/

Wayne M. Helge, Reg. No. 56,905

James T. Wilson, Reg. No. 41,439

BUNSOW DE MORY LLP

277 S. Washington St., Suite 210 #1088

Alexandria, VA 22314

T: (571) 208-0186

Email: whelge@bdiplaw.com

Email : jwilson@bdiplaw.com

Counsel for Patent Owner

CERTIFICATE OF WORD COUNT

The undersigned certifies that the foregoing PATENT OWNER'S PRELIMINARY RESPONSE complies with the type-volume limitation in 37 C.F.R. § 42.24(b)(1). According to the word-processing system's word count, the brief contains 5,127 words, excluding the parts of the brief exempted by 37 C.F.R. § 42.24(a).

By: /Wayne M. Helge/
Wayne M. Helge (Reg. No. 56,905)
Counsel for Patent Owner

CERTIFICATE OF SERVICE

I hereby certify that on December 23, 2025, a true and correct copy of the foregoing document was served via email, by consent, to Petitioner by serving the correspondence email addresses of record as follows:

<u>Lead Counsel</u> Patrick C. Keane (Reg. No. 32,858) BUCHANAN INGERSOLL & ROONEY PC 1737 King Street, Suite 500 Alexandria, Virginia 22314 Direct Telephone (703) 838-6522 Main Facsimile (703) 836-2021 patrick.keane@bipc.com	<u>Backup Counsel</u> Roger H. Lee (Reg. No. 46,317) BUCHANAN INGERSOLL & ROONEY PC 1737 King Street, Suite 500 Alexandria, Virginia 22314 Telephone (703) 838-6545 Facsimile (703) 836-2021 roger.lee@bipc.com
<u>Backup Counsel</u> Andrew J. Koopman (Reg. No. 65,537) BUCHANAN INGERSOLL & ROONEY PC 2200 Renaissance Blvd., Suite 350 King of Prussia, PA 19406 Telephone (610) 993-4217 Facsimile (610) 407-0701 andrew.koopman@bipc.com	<u>Backup Counsel</u> Samuel Harrod (Reg. No. 79,148) BUCHANAN INGERSOLL & ROONEY PC Union Trust Building 501 Grant Street Suite 200 Pittsburgh, PA 15219 Telephone (412) 562-8805 Facsimile (412) 562-1041 samuel.harrod@bipc.com

/Wayne M. Helge/
Wayne M. Helge (Reg. No. 56,905)
Counsel for Patent Owner