

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

NETSKOPE, INC.,
Petitioner,

v.

K. MIZRA LLC,
Patent Owner.

Case IPR2025-01115
Patent 8,234,705

PATENT OWNER'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	THE ’705 PATENT	5
III.	CLAIM CONSTRUCTION	8
IV.	ANALYSIS.....	10
	A. Petitioner Fails to Establish How its Proposed Combination Discloses or Suggests any Attestation of Cleanliness or a Trusted Computer Base that Ascertains Infested Status, as Required by the Challenged Claims.....	10
	B. Independent Claims 12 and 19 and the Dependent Claims are also Patentable Over Petitioner’s Challenge for the Same Reasons Stated Above	18
	C. Petitioner’s Roadmapping Falls Short	18
V.	CONCLUSION.....	20

PATENT OWNER'S EXHIBIT LIST

Exhibit No.	Description
2001	Complaint for Declaratory Judgment of Non-Infringement of U.S. Patent No. 8,234,705, <i>Netskope, Inc. v. K.Mizra LLC</i> , No. 5:25-cv-04833 (N.D. Cal.) (ECF No. 1)
2002	Declaration of Charles J. Hausman in Support of Patent Owner's Request for Discretionary Denial
2003	Screenshot of web page "Technology Partners & Integrations" (https://www.netskope.com/partners/technology-partnersintegrations , last accessed Sept. 29, 2025)
2004	Screenshot of web page "Ivanti Acquires MobileIron and Pulse Secure to Deliver Intelligent and Secure Experiences Across All Devices in the Everywhere Enterprise" (https://www.ivanti.com/company/pressreleases/2020/ivanti-acquires-mobileiron-and-pulse-secure , last accessed Sept. 29, 2025)
2005	America Invents Act, H.R. 112-98, 112th Cong. (2011)
2006	Scheduling Order, <i>K.Mizra LLC v. Google LLC</i> , 1:25-cv-00236-ADA (W.D. Tex.) (ECF No. 39)
2007	Standing Order Governing Proceedings (OGP) – Patent Cases, J. Albright (W.D. Tex.)
2008	Screenshot of Trial Statistics 01/01/2009 – 10/16/2025, U.S. District Court for the Western District of Texas
2009	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)
2010	Screenshot of Judge William P. Dimitrouleas Median Timeto-Trial Statistics, U.S. District Court for the Southern District of Florida
2011	Screenshot of Judge William P. Dimitrouleas Median Timeto-Trial with Motion to Dismiss Statistics, U.S. District Court for the Southern District of Florida
2012	Defendant Google LLC's Reply in Support of Its Motion to Dismiss Under Federal Rule of Civil Procedure 12(b)(6), <i>K.Mizra LLC v. Google LLC</i> , 1:25-cv-00236-ADA (W.D. Tex.) (ECF No. 35)

IPR2025-01115 Patent Owner's Preliminary Response

2013	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)
2014	Order Requiring Counsel to Meet, File Joint Scheduling Report and Joint Discovery Report, <i>K.Mizra LLC v. Citrix Systems, Inc. et al.</i> , No. 0:25-cv-60803-WPD (S.D. Fla.) (ECF No. 12)
2015	Google, LLC's Amended Invalidity Contentions, <i>K.Mizra LLC v. Google LLC</i> , 1:25-cv-00236-ADA (W.D. Tex.) (Aug. 5, 2025)
2016	Petition for Inter Partes Review of U.S. Patent No. 8,234,705 Under 35 U.S.C. §§ 311-319 and 37 C.F.R. §§ 42.1-100, et seq., <i>Citrix Systems, Inc. et al. v. K.Mizra LLC</i> , IPR2025-01468 (Paper 1)
2017	Patent and Trademark Office, Interim Director Discretionary Process, https://www.uspto.gov/patents/ptab/interimdirector-discretionary-process , Oct. 21, 2025
2018	Comparison of Petitions for Inter Partes Review from <i>Cisco Systems, Inc. v. K.Mizra LLC</i> (IPR2021-00593) to <i>Netskope, Inc. v. K.Mizra LLC</i> (IPR2025-01115)
2019	Comparison of Expert Declarations from <i>Cisco Systems, Inc. v. K.Mizra LLC</i> (IPR2021-00593) to <i>Netskope, Inc. v. K.Mizra LLC</i> (IPR2025-01115)
2020	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
2021	Claim Construction Order in <i>K.Mizra LLC v. Cisco Systems, Inc.</i> , No. 6:20-cv-01031-ADA (W.D. Tex.) (ECF No. 46)

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 1-3, 5-13, and 15-19 of U.S. Patent No. 8,234,705 (the “’705 patent”), as requested by Netskope, Inc. (“Petitioner”), should be denied on the merits.

I. INTRODUCTION

The ’705 patent 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.¹

The Petition challenges the claims of the '705 patent based on the proposed combination of Gleichauf (Ex. 1005), Ovadia (Ex. 1006), and Lewis (Ex. 1007). However, even if the references could be combined, the Petition still fails to demonstrate that the combination discloses all claimed elements.

In particular, as explained below, the proposed combination of prior art suffers from a failure of proof because Petitioner fails to explain how this proposed combination allegedly discloses or suggests receiving an attestation of cleanliness from a trusted computing base associated with a trusted platform module, and further fails to establish how this combination allegedly discloses or suggests a trusted computing base at a first host ascertaining whether the first host is infested, as required by the challenged claims.

In the asserted combination, Petitioner relies on Gleichauf's posture agent at a computerized device to disclose the claimed "trusted computing base" of claim 1, and relies upon a response sent from Gleichauf's posture agent to the network

¹ This aspect of the '705 patent was discussed extensively in the prior IPR filed by Cisco Systems, Inc., and should have been known by Petitioner. *See Cisco Systems, Inc. v. K.Mizra LLC*, IPR2021-00593, Paper 23 at 4-5 (PTAB Jan. 7, 2022).

policy server for the claimed “attestation of cleanliness” having “an attestation that the trusted computing base has ascertained that the first host is not infested.”

But according to Gleichauf, Gleichauf's posture agent collects credentials regarding the computerized device, and sends those credentials to the network policy server for the policy server to evaluate and determine whether those credentials comply with network policies. Importantly, per Gleichauf, it is the policy server, not the computerized device's posture agent, that evaluates the credentials sent by the posture agent and determines whether those credentials are in compliance or out-of-compliance with network policies. Petitioner fails to establish how the response from the posture agent includes an attestation of cleanliness and an ascertainment whether the first host is infested, and why a POSITA would reach such a conclusion.

Indeed, Petitioner never even undertakes an evaluation of which component in Gleichauf ascertains whether a first host is clean or infested, or how that process occurs. At most, Petitioner relies upon its expert to fill in gaps in Gleichauf regarding how a computerized device could be determined to be clean, but even this procedure invented by Petitioner's expert fails to consider what information is actually transmitted from a posture agent, how that information is used by the policy server, and how the credentials in the response message as disclosed by Gleichauf allegedly disclose the claimed features.

The Petition attempts to brush over this failure of proof in the Petition's conclusions by arguing superficially that Gleichauf's procedures are "consistent with examples of attestation of cleanliness described in the '705 patent," (Pet., 43 n.4), but even this argument fails to address differences between the disclosures of the '705 patent and Gleichauf, and just reaches the conclusion that because some of the information collected at the posture agent of Gleichauf is also mentioned in the '705 patent specification, the claimed features are satisfied. This conclusory assertion fails to address or set forth any construction related to an "attestation of cleanliness" or an ascertainment of infestation, as required by the challenged claims.

Furthermore, the Petition openly admits to roadmapping in view of a prior IPR against the '705 patent—namely, IPR2021-00593—and Petitioner goes to great lengths to explain that its challenges "provide[] further detailed analysis and evidence regarding motivations to combine" following the Board's prior decision of patentability on the '705 patent in IPR2021-00593. Pet., 4. Despite having this opportunity to evaluate a prior petition and all the associated briefing, Petitioner never turned a critical eye to the other merits shortcomings of the challenges asserted in IPR2021-00594, and therefore overlooked this substantive deficiency in its challenges. Not only did Petitioner openly roadmap its challenges, but it did so poorly. This gamesmanship should not be rewarded with institution.

As explained below, the Petitioner failed to recognize the failure of proof in its proposed combination of references. The Petition fails to explain how the asserted combination discloses or suggests every claimed feature, and this deficiency is fatal to Petitioner's obviousness challenges. 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.

III. CLAIM CONSTRUCTION

Petitioner has proposed constructions for the terms “trusted computing base” and “trusted platform module” recited in challenged claims 1, 12, and 19. Pet., 6-11. However, Petitioner offers no claim construction position on the claimed

“attestation of cleanliness” or “infested” as the proper interpretation of those terms bear on the merits of Petitioner’s challenges.

Petitioner asserts that the “trusted computing base” should be construed as “a piece of hardware or software that has been designed to be part of a mechanism that provides security to a computer system.” Pet., 8. Patent Owner does not dispute Petitioner’s proposed construction for the claim term “trusted computing base.”

For the claim term, “trusted platform module,” Petitioner relies on what it contends is an “express definition provided by the applicants during prosecution” and asserts that the term should be construed as “a secure cryptoprocessor that implements the Trusted Platform Module specification from the Trusted Computing Group.” Pet., 10. As has been determined by district court, Patent Owner contends that the proper construction of “trusted platform module” is “a secure cryptoprocessor that can store cryptographic keys and that implements the Trusted Platform Module specification from the Trusted Computing Group,” (Ex. 2021, 1) and will adopt that construction for the purposes of this IPR and POPR.

Nevertheless, the Board need not adopt a particular claim construction for either of these terms because Petitioner fails to show that the claims at issue are unpatentable for other reasons set forth below.

IV. ANALYSIS

Petitioner's challenges are based on Gleichauf,² Ovadia,³ and Lewis⁴ references. But even if combined in the manner proposed by the Petition, the Petition suffers from a failure of proof because it fails to establish that the asserted combination discloses or suggests every claimed feature. This shortcoming is fatal to the Petition.

A. Petitioner Fails to Establish How its Proposed Combination Discloses or Suggests any Attestation of Cleanliness or a Trusted Computer Base that Ascertains Infested Status, as Required by the Challenged Claims

As noted above, claim 1 of the '705 patent recites a “method for protecting a network,” where the first claimed 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*

² Ex1005, U.S. Patent No. 9,436,820 to Gleichauf *et al.* (“Gleichauf”).

³ Ex1006, U.S. Patent 7,747,862 to Ovadia (“Ovadia”).

⁴ Ex1007, U.S. Patent No. 7,533,407 to Lewis *et al.* (“Lewis”).

computing base has ascertained that the first host is not infested” Claim 1 (emphasis added).

In addressing element [1.1], the Petition first characterizes Gleichauf's computerized device 22 as the claimed “first host.” Pet., 33 (explaining that “Figure 1 of Gleichauf illustrates the computerized device 22 (*first host*) sending an access request to the 5 network 24 (*‘attempting to connect to a protected network’*).”).

The claimed “detecting” step calls back to this “first host” by also requiring that “detecting the insecure condition includes *contacting a trusted computing base associated with a trusted platform module within the first host*,” in element [1.2]. The Petition contends that “Gleichauf's computerized device includes a ‘posture agent’ and one or more ‘posture plug-ins’ installed on the device that collect information about the device's security posture.” Pet., 35. The Petition points to “the combined functionality of [Gleichauf's] posture agent and plug-ins” to disclose the claimed “trusted computing base” of claim 1. Further, Petitioner asserts that in its asserted combination of Gleichauf and Ovadia, “Gleichauf's posture agent would be augmented to implement the trusted platform module functionality, i.e., a *trusted platform module*, per Ovadia.” Pet., 39.

Based on a received response, the claimed method also requires “determining whether the response includes a valid digitally signed attestation of

cleanliness [element 1.4], 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 ... [element 1.5]" Petitioner relies upon "Gleichauf's posture agent" responding to the policy server's request as this claimed "response," and asserts that Gleichauf's posture agent sends "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." Pet., 41-42 (addressing the claimed "response"), 42-46 (addressing the claimed "attestation of cleanliness"), and 46-48 (addressing the "attestation that the trusted computing base has ascertained that the first host is not infested."). This is where Petitioner's theory of invalidity breaks down under a failure of proof.

First, Petitioner fails to analyze the disclosures surrounding Gleichauf's posture agent response to the policy server. Gleichauf makes clear that the computerized device's posture agent provides information and data regarding the computerized device in its response to the policy agent. Petitioner identifies this information as including "what particular virus software and virus definition versions are installed," "when was the last time a local antivirus scan was executed," "what operating system patches are installed," and "types and, versions of software applications" on the device. Pet., 42-43 (citing Gleichauf, 3:36-49).

But Gleichauf and Petitioner fail to substantiate Petitioner's assertion that this information is "individually and collectively" an "attestation of cleanliness."

Importantly, Petitioner fails to disclose how Gleichauf uses this information, and why this information satisfies the claimed "attestation of cleanliness."

Petitioner tries to brush over its lack of analysis in this regard by asserting that this data is "consistent with examples of attestation of cleanliness described in the '705 patent." Pet., 43 n.4. What Petitioner overlooks is that even its quoted portions of the specification of the '705 patent teach more than Petitioner recognizes. For example, even in the '705 patent quotation included in the Petition, 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); *see also* Pet. 43, n.4. Petitioner fails to point to any comparable disclosure in Gleichauf, and fails to evaluate how Gleichauf uses the data transmitted from the posture agent to the policy server. Thus, Petitioner's assertion that Gleichauf's response satisfies the claimed requirements in the '705 patent claims is conclusory and lacks support.

Indeed, in Gleichauf, as discussed below, the posture agent may report the last time a local antivirus scan was executed, but the Petition lacks any analysis regarding such disclosure. For example, Petitioner fails to consider a possibility that the last antivirus scan was out-of-date, or based on outdated virus definitions.

Per Gleichauf, the posture agent responds with this information about the computerized device, but Petitioner offers no theory how the information being transmitted from the posture agent to the policy server satisfies the claimed “response” requirements in the challenged claims.

Specifically, Petitioner fails to establish how the response from the posture agent in Gleichauf allegedly includes an “attestation that the trusted computing base has ascertained that the first host is not infested,” as claimed. The Petition points to Gleichauf’s disclosure, noting that “failure to show ‘timely execution of the anti-virus application’ is a failure to show cleanliness and results in restrictions on network access.” Pet., 46 (citing Gleichauf, 22:38-47). But Petitioner fails to disclose to the Board that in this cited portion of Gleichauf, Gleichauf discloses that this determination is made *at the network’s policy server, not the posture agent*.

Gleichauf’s specification at 22:38-47 expressly discloses that “Assume, however, that based upon the analysis, *the policy server 28 fails to detect the presence of proper configuration, or timely execution of the anti-virus application from the particular manufacturer within the accepted credential set* 46. In such an example, in one arrangement, the policy server 28 transmits a network admission instruction 48 to the data communications device 26 that directs the data communications device 26 to restrict or reject communications from the

user device 22 to the resources 25 within the network 24.” Gleichauf, 22:38-47 (emphasis added). Petitioner fails to explain how it can rely on later determinations made at the policy server to support the alleged “attestation that the trusted computing base has ascertained that the first host is not infested” being included in the response from the “trusted computing base,” as required by the challenged claim.

Petitioner also fails to consider other disclosures in Gleichauf that undercut its conclusory analysis. For example, Gleichauf expressly discloses that the policy server issues a “remediation admission policy,” and also *reports the outcome of its determinations to the posture agent*. As Gleichauf discloses:

In one arrangement, the data communications device assigns devices that are out of compliance with admission requirements to a quarantine, or remediation network. *This remediation admission policy is issued by the policy server based on comparison of the posture credentials of the device relative to predefined network admission requirements, or security policy*. At the same time the policy server determines access, the policy server can transmit one or more notification messages to the posture agent and/or posture plug-ins running on the computer device attempting the gain access to the network. The *notifications may include the results of the posture check*, remediation actions (if any) and an informational message to be displayed to the user, or written to a local log file.

Gleichauf, 4:50-63 (emphasis added). These disclosures confirm that Gleichauf's posture agent reports information and credentials to the policy server, who then performs the posture check and reports the outcome of the posture check to the posture agent via a notification. Indeed, the policy server 28 owns the analysis of the credentials collected by the posture agent. Gleichauf, 10:30-33 ("The policy server 28 is a computerized device configured to determine the particular posture credentials to request from the posture agent, and *validate the posture credentials 32* associated with the user device 22.") (emphasis added); *see also* Gleichauf, 12:14-19 ("the policy server 28 detects the presence or absence of particular anti-virus applications associated with the user device 22 and either allows or denies the user device 22 access to the network resources based upon the results of the detection."). Under these disclosures, which Petitioner does not address or consider in its analysis, Petitioner fails to establish how the response sent from the posture agent in Gleichauf to the network's policy server allegedly includes an "attestation that the trusted computing base has ascertained that the first host is not infested."

Also notable is Petitioner's use of its expert to manufacture a new process of determining cleanliness in a manner different from how Gleichauf operates. Specifically, the Petition goes outside Gleichauf to invent a new procedure, arguing that "Gleichauf expressly contemplates that failure to show 'timely

execution of the anti-virus application' is a failure to show cleanliness and results in restrictions on network access. Ex.1005, 22:38-47; Ex.1003, ¶ 132. ***It would have been obvious to a POSITA that the opposite showing would have the opposite effect.*** Ex.1003, ¶132.” Pet., 46.⁵

The claim language at issue requires “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 ...***.” Claim 1 (emphasis added). Petitioner fails to establish how Gleichauf's posture agent makes attestations of cleanliness and ascertains whether the computerized device 22 is infested. Gleichauf discloses that network's policy server owns the evaluation of the credentials sent by the posture agent to the policy server, and Petitioner never reconciles those disclosures with its alleged theory of patentability, as discussed above.

⁵ As noted above, Gleichauf's disclosures at 22:38-47 address determinations occurring at the policy server, and Petitioner fails to even attempt to explain how such determinations constitute any “ascertainment” contained within the response from the posture agent to the policy server.

Thus, even if Petitioner has established a valid motivation to combine the asserted reference (which Patent Owner disputes and will address in more detail in a Patent Owner Response if necessary), Petitioner's theory of unpatentability fails to consider or reconcile the actual disclosures of Gleichauf 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. 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 2-3 and 5-11 depend from independent claim 1, and dependent claims 13 and 15-18 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 Gleichauf, Lewis, and Ovadia.

C. Petitioner's Roadmapping Falls Short

As noted in Patent Owner's Request for Discretionary Denial, Petitioner admits that its Petition attempts to build on a previous IPR involving the same references. Pet., 4. Indeed, Petitioner explicitly attempts to fill in the potential holes in a prior petitioner's challenges through additional arguments and analysis

directed to the motivation to combine the asserted references. *Id.* (noting, in a Section titled “Discussion of Prior IPR Proceedings,” that the Petition “provides further detailed analysis and evidence regarding motivations to combine” as well as “additional mappings and discussions that were not part of the prior IPRs”). Thus, the Petition does not shy away from its roadmapping efforts, and directly responds to Patent Owner’s arguments from IPR2021-00539, directed to the same ’705 patent and based on the very same combination of references. *See* Pet., 26 n.1. Indeed, except for the roadmapped changes, the Petition and expert declaration are nearly identical to what was filed in IPR2021-00539. *See* Exs. 2018, 2019.

Notably, despite having the opportunity to review the petition filed in IPR2021-00539 and all the associated briefing surrounding that prior petition, Petitioner never turned a critical eye to how Gleichauf’s policy server behaves. Gleichauf’s policy server relies on the computerized device’s posture agent to collect and report credentials, and the policy server retains the sole decision-making power to evaluate those credentials, determine whether the computerized device is compliant or non-compliant with network policy, and then notify the computerized device’s posture agent of the result. In claim 1 (and the remaining independent claims), the first host’s trusted computing base transmits a response that includes, *inter alia*, “an attestation that the trusted computing base has

ascertained that the first host is not infested.” Petitioner fails to address how this claimed feature is allegedly disclosed given Gleichauf’s disclosures regarding the posture agent’s communications with the policy server, and fails to shore up this deficiency in its second-chance effort. Thus, not only did Petitioner clearly roadmap its challenge, but it did so without even trying to correct this failure of proof from the prior petition. The Board should deny the Petition.

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: November 21, 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 4,242 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 November 21, 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:

Thomas Millikan
Babak Tehrani
Hessam Gharaviram
Andrew Klein
Netskope-MizraIPRService@perkinscoie.com

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