

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

IRIUSRISK, INC.,
Petitioner

v.

THREATMODELER SOFTWARE INC.,
Patent Owner

IPR2023-00656

U.S. Patent No. 10,713,366

**PETITIONER'S REPLY
IN SUPPORT OF *INTER PARTES* REVIEW OF
U.S. PATENT NO. 10,713,366**

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. CLAIM CONSTRUCTION	3
A. “Threat”	3
B. “Mapping File”	5
III. GROUND 1: KEENAN ANTICIPATES THE CHALLENGED CLAIMS	7
A. Keenan Is Prior Art.....	7
1. Keenan Is Prior Art Because Keenan Is Supported By The Keenan Provisional Application.....	8
2. Keenan Is Prior Art Because The ’366 Patent Is A CIP And Is Only Entitled To A Priority Date As Of Its Filing Date Of August 15, 2019—Which Is After Keenan’s Non-Provisional Filing Date Of April 19, 2018	10
B. Keenan Discloses Threats	12
C. Keenan Discloses Dependent Claims 2-3, 9-10, 17-18	18
D. Keenan Discloses Dependent Claim 5	19
E. Keenan Discloses Dependent Claims 6 And 14.....	19
IV. GROUND 2: ZHENG IN COMBINATION WITH BAKER AND JONES RENDER THE CHALLENGED CLAIMS OBVIOUS	20
A. Zheng Discloses A Mapping File.....	20
B. It Would Have Been Obvious To Combine Zheng With Baker	23
V. CONCLUSION.....	25

PETITIONER'S EXHIBIT LIST

Exhibit No.	Description
EX-1001	U.S. Patent No. 10,713,366 (“the ’366 patent”)
EX-1002	Prosecution History of the ’366 patent
EX-1003	Declaration of Robert Hurlbut
EX-1004	U.S. Patent No. 11,200,228 (“Keenan”)
EX-1005	U.S. Patent No. 10,503,907 (“Zheng”)
EX-1006	U.S. Patent Pub. 2014/0236665 (“Baker”)
EX-1007	U.S. Patent No. 9,602,529 (“Jones”)
EX-1008	U.S. Patent No. 10,681,068 (“Galliano”)
EX-1009	Federal Judiciary Report
EX-1010	Email from Petitioner’s Counsel to PO’s Counsel
EX-1011	Excerpts from <i>Risk Centric Threat Modeling</i> , by Tony Uceda Velez and Marco M. Morana, John Wiley and Sons, Inc., 2015
EX-1012	Excerpts from <i>Threat Modeling Designing for Security</i> , by Adam Shostack, John Wiley and Sons, Inc., 2014
EX-1013	Excerpts from <i>Threat Modeling</i> , by Frank Swiderski and Window Snyder, Microsoft Press, 2004
EX-1014	Excerpts from <i>The Security Development Lifecycle</i> , by Michael Howard and Steve Lipner, Microsoft Press, 2006
EX-1015	Deposition Transcript of Dr. Seth Nielson
EX-1016	Supplemental Declaration of Robert Hurlbut
EX-1017	U.S. Patent No. 10,699,008
EX-1018	Redline Between Specifications of the ’366 and ’008 patents
EX-1019	U.S. 62/487,370 Keenan Provisional
EX-1020	Claim Chart Comparing Claim 1 of Keenan to the Keenan Provisional
EX-1021	Claim Chart Comparing Claims 1-20 of the ’366 Patent to the Keenan Provisional

Exhibit No.	Description
EX-1022	Claim Chart Demonstrating the Portions of Keenan Petitioner Relies Upon Are Supported by the Keenan Provisional
EX-1023	European Windstorms, https://en.wikipedia.org/wiki/European_windstorm
EX-1024	4 Key Characteristics of Risk Explained (+ Examples)

IriusRisk Inc. ("Petitioner") submits this reply to ThreatModeler Software Inc.'s ("PO") Patent Owner Response ("POR") (Paper 19) in support of Petitioner's Petition for *Inter Partes* Review ("Petition") (Paper 1).

I. INTRODUCTION

PO's only argument as to why Keenan does not anticipate the independent claims of the '366 patent is that Keenan does not disclose "threats" because Keenan only discloses risks, and threats and risks are different concepts.¹ POR, 29-41. But this was never in dispute—IriusRisk's Petition acknowledges threats and risks are different and instead argues that a POSITA would understand that Keenan discloses threats as well as risks (Petition, 21-24 ("A POSITA would understand that Keenan's 'risk' includes threats because measuring risk includes a determination of threats"), 26-28 (same))—a fact that the POR hardly addresses.

Indeed, the fact that a POSITA would understand that a risk analysis such as the one disclosed in Keenan includes threats is beyond dispute. EX-1015 (transcript for deposition of PO's expert witness), 9:22-10:7 ("a ***risk analysis requires some form of threat analysis***, and then based on the threat analysis, you assess risk that's either quantitative, or it can be qualitative, as in you can prioritize the risk. ***But it's based on assessment of threats.***"). Both sides' experts agree that

¹ The POR also includes separate arguments directed to why Keenan does not meet the dependent claims of the '366 patent.

the definition of “risk” is the likelihood of the threat occurring multiplied by the impact of that threat. EX-2002, 24:3-25:5, 31:5-33:2; EX-1015, 61:8-62:12 (this definition “is the way I’ve been using ‘risk,’ both in my career and in this patent.”). This definition requires an understanding of the threat to understand both “likelihood” and “impact.” Importantly, Keenan discloses performing this calculation. EX-1004, 18:6-22. And since threats are part of Keenan’s analysis, Keenan discloses storing those threats in its system. EX-1004, 6:56-60 (“Effectively, if data, destined for inclusion in analysis or reporting, is held in a location then a data storage object must exist.”).

PO’s remaining arguments relate to the combination of Zheng and Baker in Ground 2. Although the Board preliminarily found that Zheng’s mapping relates solely to cartography, the expert testimony in this case, including from PO’s expert, Dr. Nielson, demonstrates that the Board applied a too narrow understanding of Zheng’s mapping. Specifically, Zheng applies a simple cartographic mapping to the base layer that displays the application architecture, but then overlays additional layers—including a threat modeling layer—that are “in addition to basic cartographical details.” EX-1005, 4:13-16; EX-1015, 128:14-21 (“traffic” and Zheng’s overlays “active attacks on top of the system architecture” are examples of things “beyond basic cartographic details.”). Zheng’s system then uses a database table—which the ’366 patent acknowledges is

a type of mapping file (EX-1001, 38:33-42)—to link or “correlate” each layer.

EX-1005, 8:25-38; EX-1015, 123:21-124:19.

The Board should find claims 1-20 unpatentable.

II. CLAIM CONSTRUCTION

A. “Threat”

Petitioner's definition of a “threat” is an “undesirable event that may happen.” EX-2002, 19:17-25. PO's alternative definition of a threat as “one or more potential events that, if they occur, can cause adverse effects to a target system” (EX-2009, ¶78) is essentially the same as Petitioner's definition. Indeed, there is no meaningful difference between an “undesirable event” and “potential events that ... can cause adverse effects to a target system.” However, PO's definition is slightly incorrect because the words “if they occur” remove all consideration of whether the event is likely to occur, leading to the absurdity that an event that is impossible can still be considered a “threat” because the words “if they occur” requires one to ignore that impossibility. This aspect of PO's construction is directly contrary to the testimony of PO's expert, Dr. Nielson, and the specification of the '366 patent.

As confirmed by PO's expert, Dr. Nielson, what is considered a “threat” depends on context. EX-2002, 27:19-29:5, 59:4-16 (“identifying threats does depend a little bit on how you're modeling it.”). For example, when asked if

bluejacking is a threat to a Bluetooth port on a laptop, Dr. Nielson testified that “it could be” because “it would have to take some context into consideration,” such as the “type of data you [are] trying to protect,” “the way you use your laptop,” and “where you use your laptop.” *Id.* In other words, bluejacking may not be a threat in certain situations, such as if it is impossible for bluejacking to occur. Indeed, as Dr. Nielson points out, this is why the ’366 patent says that bluejacking “may” be a threat. *Id.*, 28:20-29:5; EX-1001, 10:8-21. Thus, the context influences whether the undesirable event “may happen.”

But, under PO’s definition, “bluejacking” would always be a threat because bluejacking is an event that, if it occurs, will cause adverse effects to a target system. PO’s definition thus does not allow for contextual situations where the threat will not occur and instead assumes that an event “if it occurs” and will cause adverse effects to a target system, then that event is a threat. Under PO’s definition, any event that can cause adverse effects to a target system can be a threat—even if it is impossible for that threat to occur. For example, even if a laptop does not have a Bluetooth port, “bluejacking” would still be a threat under PO’s definition because “if it occurs,” it will cause adverse effects to the target system. This is contrary to Dr. Nielson’s testimony and the ’366 patent. EX-2002, 27:19-29:5; EX-1001, 10:8-20.

Thus, the definition of “threat” is an “undesirable event that may happen” as proposed by Petitioner. EX-2002, 19:17-25. In any event, as explained below in Section III.B, the Keenan reference includes threats under either party’s definition.

It is also important to understand that, under either party’s definition, a POSITA may use alternative framings of what event is a “threat” and what is an “adverse effect” (or an “undesirable” event) depending on the “context” including “what it is you’re trying to protect and what properties you need to maintain.” EX-2002, 48:16-22 (“adverse effects is also context-dependent.”); *see also id.* 28:3-13, 58:8-59:16 (threats can be identified at a high level depending on how the threats are modeled). For example, a POSITA threat modeling for an insurance company might frame “freeway collisions” as the threat (EX-1001, 9:66-10:7) and damage to a car as the adverse effect in order to study the effects of freeway collisions on premiums. But, under a different framing, a POSITA may frame “drunk driving” as the threat and “freeway collision” as the adverse effects if attempting to model the number of freeway accidents caused by drunk driving.

B. “Mapping File”

Mapping files are general terms that are well known to POSITAs in the field of threat modeling. EX-2002, 26:22-24 (“A mapping file is actually a general term that's well-known for those who are skilled in the art”). Thus, under the plain and ordinary meaning of the term, a POSITA would understand that a “mapping file”

as “a file or other representation that correlates data from a source to a target.”

Id., 26:17-27:25 (“the purpose of the mapping file is to correlate data from a source to a destination”).

PO’s definition of a “mapping file” as “a file or one or more tables that correlate threat model components with visual diagram components of a third party software application” (POR, 28) applies an unduly restrictive definition of “mapping file” that imports other language from the claim into the construction of the term. Specifically, the portion of PO’s definition reciting “correlate threat model components with visual diagram components of a third party software application” is language recited elsewhere in the claims. *E.g.*, EX-1001, 43:30-35. This is improper as it is inconsistent with the plain and ordinary meaning of “mapping file.” Indeed, adopting PO’s definition would render other claim language redundant, which is also improper. *See Robotic Vision Sys., Inc. v. View Eng’g, Inc.*, 189 F.3d 1370, 1376 (Fed. Cir. 1999) (rejecting a construction on the ground that it “would necessarily be redundant and would add no additional limitations.”); *Fortinet, Inc. v. Sophos, Inc.*, 2015 WL 877410, at *13 (N.D. Cal. Feb. 27, 2015) (rejecting proposed construction because “the limitations requested by Fortinet already appear in the relevant claims, and thus its requested construction is redundant.”).

Moreover, PO did not act as its own lexicographer by explicitly defining “mapping file.” *See generally* EX-1001. Thus, PO provides no reason why a “mapping file” should be construed more narrowly than its plain and ordinary meaning. *Johnson Worldwide Associates. Inc. v. Zebco Corp.*, 175 F.3d 985, 989 (Fed. Cir. 1999) (when the patent applicant is not deemed to be his own lexicographer, claim terms are given their “ordinary and accustomed meaning.”). Although the claims of the ’366 patent define that the mapping file is used to “correlate threat model components with visual diagram components of a third party software application,” the plain and ordinary meaning of a “mapping file” is broader than these other limitations included within the claims of the ’366 patent. EX-2002, 26:22-24 (“A mapping file is actually a general term that's well-known for those who are skilled in the art”).

III. GROUND 1: KEENAN ANTICIPATES THE CHALLENGED CLAIMS

A. Keenan Is Prior Art

As discussed in more detail in Section III.B., PO’s only substantive argument that Keenan does not anticipate the challenged independent claims is that Keenan only discloses risk analysis, not the claimed “threats.” But there is no reasonable dispute that Keenan’s risk analysis discloses threats because, among other reasons, “a *risk analysis requires some form of threat analysis.*” EX-1015, 9:22-10:7; *see also* Section III.B. After failing to raise any genuine substantive

disputes to Petitioner's anticipation challenge, PO resorts to arguing that Keenan is not prior art, but PO is wrong for two reasons: (1) Keenan's non-provisional is supported by its provisional application U.S. Provisional Patent App. No. 62/487,370 (the "Keenan Provisional") (EX-1019); and (2) the '366 patent is a CIP and is only entitled to a priority date as of its filing date of August 15, 2019—which is after Keenan's non-provisional filing date.

1. Keenan Is Prior Art Because Keenan Is Supported By The Keenan Provisional Application

Preliminarily, PO is wrong that "it would be improper for Petitioner to supplement the record by trying to show that the relevant portions of Keenan are entitled to Keenan's provisional filing date." POR, 48. Federal Circuit law is "very clear" that it was PO's burden to challenge the prior art status of the Keenan reference. *Innovative Growers Equip., Inc. v. Pipp Mobile Storage Sys., Inc.*, No. IPR2022-00893, 2023 WL 7107846, at *18 (P.T.A.B. Oct. 27, 2023) ("*Dynamic Drinkware* is very clear on this point. The petitioner in an *inter partes* review does not have the burden of producing evidence that the effective date of an asserted reference patent relates back to its claimed provisional application until after a patentee challenges the prior art status of the asserted reference. ... Thus, Petitioner did not waive any argument by asserting in its Petition that Hutto was entitled to its claimed earlier effective date" in its provisional application), citing *Dynamic Drinkware, LLC v. National Graphics, Inc.*, 800 F.3d 1375, 1381 (Fed.

Cir. 2015) (“[I]t was not necessary for Dynamic to prove in its petition that Raymond was entitled to the filing date of its provisional application.”).

To claim priority from the Keenan Provisional: (1) the provisional application must support at least one claim of Keenan and (2) the disclosure of Keenan must have been carried forward from the Keenan Provisional. *Dynamic Drinkware*, 800 F.3d at 1380-81.

First, the Keenan Provisional (EX-1019) supports at least one claim of the Keenan patent. This is shown in Mr. Hurlbut's Supplemental Declaration (EX-1016) and the chart he prepared that explains how each limitation in claim 1 of Keenan is supported by the Keenan Provisional (EX-1020). *See* EX-1016, ¶¶7-10; EX-1020.

Second, the disclosures of the Keenan patent relied on in the Petition were carried forward from the Keenan Provisional. Indeed, the Keenan Provisional has identical figures and a highly similar detailed description to the Keenan patent. *Compare* EX-1004 *with* EX-1019. For the avoidance of doubt, reproduced as EX-1022 is the claim chart initially attached to Mr. Hurlbut's declaration (EX-1003 at Exhibit B) except with citations to the Keenan Provisional. Also included as EX-1021 is a claim chart showing that claims 1-20 of the '366 patent are met by the Keenan Provisional in the same manner as the Keenan patent. These charts

demonstrate that the disclosures in the Keenan patent that the Petition relies upon were carried forward from the Keenan Provisional. *See also* EX-1016, ¶¶11-13.

2. Keenan Is Prior Art Because The '366 Patent Is A CIP And Is Only Entitled To A Priority Date As Of Its Filing Date Of August 15, 2019—Which Is After Keenan's Non-Provisional Filing Date Of April 19, 2018

Keenan is also prior art because the Keenan patent was filed on April 19, 2018, which is eight months before the earliest possible priority date of the '366 patent of August 15, 2019. Petitioner previously assumed that the priority date of the '366 patent was May 17, 2017 simply because there was no reason to challenge the '366 patent's priority date—after all, all of Petitioner's prior art predated the May 17, 2017 date. Petition, 8. But now that PO has challenged the date of the prior art, Petitioner fairly responds to PO's argument by challenging the '366 patent's priority date. *Cf. United Therapeutics Corp. v. Liquidia Techs., Inc.*, 2023 WL 8794633, at *3 (Fed. Cir. Dec. 20, 2023) (affirming Board's finding "that [Petitioner's] arguments and evidence raised in its Reply were not untimely as they were made in direct response to [Patent Owner's] attack on the prior art status of the abstracts first raised in its post-institution Patent Owner Response.").

The '366 patent filed on August 15, 2019 is a continuation-in-part of U.S. Patent Application No. 16/228,738, filed on December 20, 2018 (the "Parent Application") and issued as U.S. Patent No. 10,699,008. *See* EX-1001; EX-1017; EX-1016, ¶4. Claims 1-20 of the '366 patent all require a "mapping file" used for

“correlating the threat model components with visual diagram components of a third party software application.” EX-1001; EX-1016, ¶5.

But the Parent Application does not include any reference to a “mapping file” used for “correlating the threat model components with visual diagram components of a third party software application” claimed by all claims of the ’366 patent. EX-1016, ¶6. Included as EX-1018 is a redline between the Parent Application and the ’366 patent. As shown in EX-1017 and EX-1019, figures 23-29 of the ’366 patent and their related descriptions are entirely new to the ’366 patent. EX-1001, 35:21-43:11, Figs. 23-29; EX-1016, ¶6. These newly-added figures and descriptions relate to the concept of a “mapping file” used for “correlating the threat model components with visual diagram components of a third party software application.” EX-1016, ¶6. Additionally, the Parent Application also does not disclose “visual diagram components of a third party software application.” *Id.*

Thus, the Parent Application does not convey to a person of ordinary skill in the art that the inventor had possession at the time the Parent Application was filed of the “mapping file” or “visual diagram components of a third party software application” recited in claims 1-20 of the ’366 patent. *Id.* This means that claims 1-20 of the ’366 are not entitled to the filing date of the Parent Application as their priority date and that their priority date instead is the filing date of the ’366 patent

on August 15, 2019. As such, since the Keenan patent non-provisional was filed on April 19, 2018—months before the priority date of the '366 patent—Keenan is prior art under at least pre-AIA 102(a).

B. Keenan Discloses Threats

PO's only substantive argument that Keenan does not anticipate the challenged independent claims is that Keenan does not disclose "threats" because Keenan only discloses "risk." POR, 18-25, 29-41. But there is no dispute that a POSITA would understand that "*a risk analysis requires some form of threat analysis.*" EX-1015, 9:22-10:7. Thus, although threats and risk are different concepts, it is undisputed by the parties' experts that Keenan's risk analysis requires an underlying threat analysis. *Id.*

Indeed, the definition of risk applied by both parties confirms that a risk analysis includes an understanding of the underlying threat. The definition of "risk" that PO's expert Dr. Nielson applied in his report is "the potential impact on a system *due to a threat* that occurs coupled with the *likelihood that a threat will occur.*" EX-1015, 61:8-62:12 ("likelihood times impact is the way I've been using 'risk,' both in my career and in this patent."); *see also* EX-2009, ¶¶80-86 (applying this definition and citing a multitude of exhibits applying this same definition); POR, 19-24, 30 (same); EX-2003 ("Risk = Likelihood x Impact."); EX-2006, B-9 (risk is "[a] measure of the extent to which an entity is threatened"); EX-2007, 109,

127; EX-1002, 493. Petitioner's expert, Mr. Hurlbut, agrees with this definition of risk. EX-2002, 24:3-25:5, 31:5-33:2.

Under this definition, a POSITA must determine the threat to understand both the “impact” and “likelihood” of that threat when calculating risk. Realizing that this definition necessarily means that Keenan's risk analysis includes threats, Dr. Nielson attempted to run from this definition at his deposition. *Compare* EX-1015, 61:8-62:12 (“Q And that's the definition you applied in your report? A Yes.”) *with id.*, 88:9-89:22 (“Q ... your definition of risk is the likelihood of a threat by the impact of that threat; is that correct? A No.”). Dr. Nielson's about face to salvage PO's position lacks credibility, particularly where Dr. Nielson testified that the “likelihood X impact” definition was the one he applied in his report (and in his career). EX-1015, 61:8-62:12; *see also* EX-2009, ¶¶80-86 (applying this definition and citing a multitude of exhibits applying this same definition).

Dr. Nielson's testimony also lacks credibility where he attempts to use his definition of “threats” narrowly—stripped of all context—to argue that risk can exist without threats. As discussed above, what event is considered a “threat” and what is an “adverse effect” depends on context, including “what it is you're trying to protect and what properties you need to maintain.” EX-2002, 48:16-22 (“adverse effects is also context-dependent.”); EX-2002, 27:19-29:5 (threats

depend on context), 58:14-59:16 (“identifying threats does depend a little bit on how you're modeling it.”); Section II.A. For example, Dr. Nielson provides an exemplary scenario where an insurance company is selling life insurance, the threat is “the causes of death.” EX-2009, ¶106.² But, analyzing context, *i.e.*, what the insurance company is actually trying to protect (its bottom line), the threat is not “causes of death,” but actually a policyholder dying at a certain time causing a loss. *See* EX-1015, 104:1-20.

Importantly, this definition of “risk” is also consistent with Keenan, which discloses calculating risk. For example, Keenan “allows the user a quick way to calculate the risk of the selected View.” EX-1004, 18:6-22. As discussed, a POSITA would understand that Keenan calculates this risk by multiplying “the potential impact on a system *due to a threat* that occurs” with “the *likelihood that a threat will occur*.” *See* EX-1015, 61:8-62:12; EX-2002, 24:3-25:5, 31:5-33:2. An understanding of the “threat” is on both sides of this equation—and thus an integral part of Keenan’s risk analysis. Keenan further discloses that all parts of its analysis are stored in its system. EX-1004, 6:56-60 (“Effectively, if data, destined for inclusion in analysis or reporting, is held in a location then a data storage object

² Despite including this scenario in his report, Dr. Nielson testified at his deposition that he could not identify the event that leads to the risk (*i.e.*, the threat) because he is not an insurance expert. EX-1015, 103:8-104:20 (“I’m not sure at this point. You’re reaching the end of my understanding as an insurance expert, as I’m not one.”).

must exist.”). Thus, all record evidence demonstrates that Keenan stores threats as part of its risk analysis.

A close review of Keenan further confirms that Keenan discloses threats as part of its analysis. For example, Keenan discloses using color to categorize risk based on the type of risk (*i.e.*, cyber, environmental, accidental). EX-1004, 16:40-51; Petition, 28; EX-1003, ¶79. These “types of risk” stem from the underlying threat—*i.e.*, cyber threats, environmental threats, and accidental threats. In other words, as discussed above, “risk” does not exist in a vacuum, and therefore specific types of risk stem from specific types of threats. EX-1015, 101:21-133:4. Indeed, like Keenan, the ’366 patent discloses organizing the composition of threats by the type of risk. EX-1001, 24:53-58 (“the composition of threats by risk type”).

In the Institution Decision, the Board agreed that this disclosure identifies threats, finding that “Patent Owner then merely concludes, without citing any factual support, that use of a color identifying the generic nature of a risk still fails to disclose any threats associated with the risk.” Institution Decision, 18-19. In response, PO provides a single conclusory statement that: “the use of color identifying risk levels is not the same as teaching the presence of threats. Patent Owner’s expert agrees.” POR, 37-38. But PO notably ignores that the use of color in Keenan is not merely identifying “risk level”—it is identifying “the *generic*

nature of a risk,” which identifies the nature of the threat, as discussed above.

EX-1003, ¶¶79, 82.

PO also argues that Keenan’s disclosure of “cyber, environmental, accidental, etc.” identifies risk only, not threats. POR, 40-41. But again, identifying “types of risk” serves to also identify the underlying type of threat. Dr. Nielson admitted as much at his deposition: “cyber risk and environmental risks [in Keenan] relate to risks from different types of problems.” EX-1015, 102:11-16. And when asked how to determine “types of risk” in Keenan, Dr. Nielson testified that the type of risk comes from the threat, such as if “I have electronically stored data that is somehow stolen, you know, that’s data that’s stored in cyberspace.” EX-1015, 102:17-130:4 (“obviously there are some bright-line distinctions.”). Indeed, both parties’ experts had no trouble identifying various types of problems that may arise from cyber, environmental, and accidental risks at their depositions. EX-2002, 61:7-24 (identifying threats from hypothetical risk); EX-1015, 51:12-14 (freeway collision can be an “accidental” threat), 57:4-60:19 (malware, phishing, and DDOS are types of cyber threats), 102:17-130:4, 105:11-106:6.

And to the extent that PO argues the disclosure in Keenan of “cyber, environmental, accidental” threats does not identify the specific threat, this is wrong for three reasons. First, there is simply no requirement in the claims of the ’366 patent that a specific threat must be identified. *See* Institution Decision,

19 (“‘threats’ is broadly recited in claim 1 with no requirement as to any level of specificity of such threats.”). PO presents no evidence to the contrary. Indeed, PO’s expert Dr. Nielson testified that threats can be identified at a high level because “identifying threats does depend a little bit on how you're modeling it.” EX-1015, 58:14-59:16.

Second, as explained above, a POSITA presented with a threat or risk category would understand at least some of the specific underlying threats. Indeed, both parties’ experts readily identified threats that may arise from types of risks at their depositions. EX-2002, 61:7-24 (identifying threats from hypothetical risk); EX-1015, 51:12-14, 57:4-60:19, 102:17-130:4, 105:11-106:6.

Third, Keenan does identify specific threats. For example, Keenan discloses an example of a model named “European Windstorm Model.” EX-1004, 9:42-47. A European windstorm is a specific type of natural disaster. EX-1023. A POSITA would understand that natural disasters are threats that could be included in a threat model. EX-1015, 53:1-10, 84:3-20. And, as confirmed by PO’s expert Dr. Nielson, a risk model may be narrowed such that it identifies a single threat. EX-1015, 84:3-20. For example, a risk model analyzing the risk of “Atlantic hurricanes in the United States” identifies the hurricane as the threat. *Id.* (“You could narrow a model down, a risk model down to where this was only one potential threat that is being identified.”). Likewise, Keenan discloses a model

identifying a specific threat: European windstorms. And since the European windstorm is part of Keenan's analysis, this threat is stored in Keenan's system. EX-1004, 6:56-60 ("Effectively, if data, destined for inclusion in analysis or reporting, is held in a location then a data storage object must exist.").

Yet another way that Keenan discloses threats is Keenan's disclosure of mitigating resulting risk. EX-1004, 20:22-33. A POSITA would understand that risks cannot be mitigated without mitigating the threat. EX-1015, 75:1-17. And a still further way that Keenan discloses threats is through "risk characteristics"—one of which is threats. EX-1003, ¶82; EX-1024 (identifying "source," "impact," and "likelihood" as characteristics).

PO attempts to obfuscate these disclosures of threats by arguing that Keenan's main focus is risk assessment (POR, 29-30) and that Keenan is assigned to an insurance company (POR, 11-12 ("The purpose of Keenan is to provide a view ... for business and insurance purposes")), but these facts are irrelevant. Keenan still discloses threats for the reasons discussed above. Thus, Keenan anticipates the challenged claims.

C. Keenan Discloses Dependent Claims 2-3, 9-10, 17-18

Claims 2, 9, and 17 require that the mapping file is stored on "the one or more computing devices." Keenan discloses these claims because Keenan discloses—in the second-to-last paragraph of the specification—that "*all* or a part

of steps of the processes in the preceding embodiments is preferably implemented by relevant computing hardware instructed by a program,” which “may be stored in a computer readable storage medium.” EX-1004, 21:27-33; EX-1003, ¶109; Petition, 41-42. PO presents a conclusory argument that this disclosure does not apply to the mapping file (POR, 43), but this is plainly wrong because Keenan is explicitly referring to “all” of the preceding embodiments, including the mapping file.

For Claims 3, 10, and 18 PO does not address that Petition's argument that Keenan teaches a “characteristics table” with “Flow Objects” that allow a user to make connections on the screen of the GUI. Petition, 42; POR, 41-44.

D. Keenan Discloses Dependent Claim 5

PO does not dispute that Keenan discloses the steps of claim 5, but merely that Keenan discloses them in the wrong order. POR, 44-45. But PO wholly ignores the Petition's argument that “a POSITA would further understand that Keenan discloses a system that checks for default titles or user-defined name matches in either order.” Petition, 43-44.

E. Keenan Discloses Dependent Claims 6 And 14

PO again ignores the Petition's actual arguments (1) that “[a] POSITA would understand that Keenan's system creates a placeholder component where no exact match is found for the third party component object the user adds to

Keenan's IOE, and then displays that placeholder in the IOE, indicating no match was found"; and (2) that a POSITA would understand Keenan's disclosure of temporary topology in memory discloses this claims. Petition, 45-47.

IV. GROUND 2: ZHENG IN COMBINATION WITH BAKER AND JONES RENDER THE CHALLENGED CLAIMS OBVIOUS

A. Zheng Discloses A Mapping File

Although the Board preliminarily found that Zheng's mapping relates solely to cartography, the expert testimony in this case, including from PO's expert, demonstrates that the Board applied a too narrow understanding of Zheng's mapping. EX-1015, 128:14-21 ("traffic" and Zheng's overlays "active attacks on top of the system architecture" are examples of something "beyond basic cartographic details.").

Zheng only uses the term "cartography" twice in its entire specification—and both uses make clear that "cartography" is not the sole type of mapping disclosed by Zheng's system. First, Zheng discloses cartography as one exemplary approach to mapping application architecture. EX-1005, 3:28-31 ("by utilizing a visualization approach like cartography, application architecture can be represented."). As the Board correctly noted, the remainder of Zheng's specification is consistent that the "application architecture" can be represented by mapping techniques like cartography.

What the Board misunderstood, however, is that this application architecture is only the ***base layer*** of Zheng's system. EX-1005, 3:66-4:2 ("the multilayered structure 200 includes four different overlaying layers, with the base layer 202 representing at least a portion of a company's application architecture."). Zheng in fact discloses a multi-layered structure, where additional layers that overlay the base layer include "a layer representing threat modeling 204 of perceived threats," among other layers. EX-1005, 4:7-16.

These layers overlay the base layer and provide details that are "***in addition to basic cartographical details.***" EX-1005, 4:13-16; EX-1015, 128:14-21. Specifically, the layers are linked or mapped together to provide additional details that overlay on the architecture of the base layer—and this linkage goes far beyond simple cartography. For example, the threat modeling layer overlays the application architecture of the base layer and identifies which applications in the architecture are "threat targets" for potential threats. EX-1005, 5:6-24 ("the visualization module 116 generates and renders the threat modeling layer 204 in a computer display to visualize predicted security objectives, threats and/or vulnerabilities of the application architecture in the base layer 202. ... Each threat can be visually associated with at least one of (i) a threat actor application, (ii) a threat target application and (iii) a displayable vector connecting the two to represent and visualize a particular attack methodology."); EX-1015, 128:14-21

(“traffic” and Zheng’s overlays “active attacks on top of the system architecture” are examples of things “beyond basic cartographic details.”). Specifically, the application architecture in the base layer are not identified as threat target applications until a user overlays the threat modeling layer, linking threats and threat target applications to the application architecture—a process Zheng also refers to as mapping. *See* EX-1005, 5:18-24 (“A threat can provide one-to-one mapping between a threat actor and a threat target.”); EX-1015, 120:2-22.

Indeed, a visualization structure that uses overlaying layers is quite different than the simple practice of drawing a cartographic map. *See* EX-1015, 127:2-128:21. It is this overlay linkage between layers or “map” that the Petition relied upon for Zheng’s mapping because it is the threat modeling layer that overlays the threats and threat actors on the base layer. Petition, 63 (citing, *e.g.*, 5:18-24); EX-1003, ¶160 (discussing threat modeling layer’s visualizations).

Importantly, Zheng discloses the use of a mapping file for interactions between the layers: Zheng discloses that a database table may be used to store data for each layer and for each possible combination and interaction of the layers. EX-1005, 8:25-38 (“at least one database table is used to store data for each layer and for each possible combination/interaction of the layers.”); EX-1015, 123:21-124:19 (Zheng “discusses creating a database table[] that represent interactions between” layers). The ’366 patent explicitly acknowledges that a database table is a type of

mapping file. EX-1001, 38:33-42 (where “one or more tables of the database are used for the mapping file(s), each table is, for the purposes of this disclosure, a “file.”). Thus, Zheng’s disclosure of a database table that “correlates data from a source to a target” (*i.e.*, between the base layer and threat modeling layer) is a mapping file. Section II.B.

B. It Would Have Been Obvious To Combine Zheng With Baker

First, Baker’s system also discloses a mapping file. Baker discloses using shapes to represent components of its native system. EX-1006, ¶[0025] (“As are understood by persons involved in risk management processes, a risk management flowchart utilizes symbols of various shapes to indicate actions, determinations, or other elements of an activity or evaluation”). Baker then discloses importing third party visual diagram components (*i.e.*, Visio shapes and flowcharts) into its system, which are used in place of Baker’s native shapes and formats. *Id.* (“At step 106, the processor 20 acts to automatically assign or associate predetermined objectives or controls according to the shapes of the imported flowcharts.”). In other words, Baker correlates native components with imported components, *i.e.*, correlate “components with visual diagram components of a third party software application” as claimed. A mapping file is needed to do so because of the differences between Baker’s native code and the code of the imported Visio diagrams. *See* EX-1015, 132:6-134:17.

Second, it would have been obvious to combine Baker's ability to import Visio shapes and formats and correlate those third party diagram shapes with shapes of the native system. Preliminarily, the Petition's use of Baker for Element 1[d] was not an affirmation that Zheng does not disclose "mapping techniques" in the context of "correlating" components (Institution Decision, 27); rather, Zheng practices correlating as described above (and even discloses importing from different "sources" (Petition, 64-65; EX-1003, ¶165)), and it would have been obvious to use Baker's correlating Visio shapes to native shapes in Zheng's system. Petition, 64-65.

The obviousness of such a combination and the motivation to combine and expectation of success of such a combination is beyond dispute. Petition, 64-65. The ability to import visual diagram components of a third party software is well known in the art. The '366 patent itself admits this fact. EX-1001, 2:47-54 (Lucidchart is an example of a program that "will convert a MICROSFOT VISIO file into another file type (for example importing the visual elements and retaining some diagram features of the original VISIO file)."). Although the '366 patent's claim to novelty is that such a feature had not been used in threat models before (not true), this does not render the claims non-obvious. Moreover, Dr. Nielson confirmed that one could draw a threat model in a program such as Lucidchart (or a similar program), and then import Visio shapes into that program—thus

importing visual diagram components of a third party software into that threat model—the exact feature the '366 patent claims is not found in the prior art. EX-1015, 30:10-31:1, 32:19-35:13.

Dr. Nielson also confirmed that this feature is well known, testifying that he “wouldn’t be surprised” if another software program, such as Lucidchart, had the ability to import Visio shapes because such a feature was so well known in the art. EX-1015, 33:9-15 (“A lot of charting tools have ways of converting a chart from one form to another.”).

V. CONCLUSION

Petitioner has shown that claims 1-20 are unpatentable and thus requests cancellation of these claims.

Respectfully submitted,

Dated: March 29, 2024

/Brent Yamashita/
Brent Yamashita

CERTIFICATION OF WORD COUNT

Pursuant to 37 C.F.R. § 42.24(c) and (d), Petitioner certifies that the word count of Petitioner's Reply in Support of its Petition for *Inter Partes* Review (exclusive of any table of contents, table of authorities, certificates of service and word count, and list of exhibits or claim listing) as measured by Microsoft Word is 5,587 words.

By: /Brent Yamashita/
Brent Yamashita

**CERTIFICATE OF SERVICE ON PATENT OWNER
UNDER 37 C.F.R. § 42.105**

Pursuant to 37 C.F.R. §§ 42.6(e) and 42.105(b), the undersigned certifies that, on March 29, 2024, a complete and entire copy of this Reply in Support of its Petition for *Inter Partes* Review, together with all supporting exhibits, were served on Patent Owner electronically, by agreement, by emailing a copy of the same to the following attorneys for the Patent Owner:

djackson@dbjg.com
Donald.jackston@rimonlaw.com
mkaufman@reedsmith.com
marc.kaufman@rimonlaw.com

By: /Brent Yamashita/
Brent Yamashita