

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.,
Petitioner,

v.

CROGA INNOVATIONS LTD.,
Patent Owner.

IPR2024-01283
Patent 11,223,601 B2

Before TERRENCE W. McMILLIN, JOHN R. KENNY, and
RUSSELL E. CASS, *Administrative Patent Judges*.

McMILLIN, *Administrative Patent Judge*.

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

I. INTRODUCTION

A. *Background and Summary*

Cisco Systems, Inc. (“Petitioner”)¹ filed a Petition for *inter partes* review of claims 1–16 of U.S. Patent No. 11,223,601 B2 (Ex. 1001, “the ’601 patent”). Paper 2 (“Pet.”), 9. Croga Innovations Ltd. (“Patent Owner”)² filed a Preliminary Response. Paper 7 (“Preliminary Response” or “Prelim. Resp.”).

Patent Owner’s Preliminary Response does not address the merits of Petitioner’s challenges to patentability. *See generally* Prelim. Resp. The only issue raised in the Preliminary Response is discretionary denial in light of a parallel district court case. *Id.*

We have authority to determine whether to institute an *inter partes* review. 35 U.S.C. § 314 (2018); 37 C.F.R. § 42.4(a) (2020) (“The Board institutes the trial on behalf of the Director.”). The standard for institution is set forth in 35 U.S.C. § 314(a), which provides that *inter partes* review may not be instituted unless “there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” After considering the Petition and the Preliminary Response, as well as the evidence of record, we institute an *inter partes* review as to claims 1–16 of the ’601 patent.

B. *Related Proceeding*

The parties identify the following district court matters related to the ’601 patent: *Croga Innovations Ltd. v. Cisco Systems, Inc.*, No. 2-24-cv-

¹ Petitioner identifies itself Cisco Systems, Inc. as the real party-in-interest to this proceeding. Pet. 109.

² Patent Owner identifies itself Croga Innovations Ltd. as the real party-in-interest to this proceeding. Paper 5, 2.

00065 (E.D. Tex.); and *Croga Innovations Ltd. v. Palo Alto Networks, Inc.*, No. 2-24-cv-00208 (E.D. Tex.). Pet. 109; Paper 5, 2; Paper 6, 2; Paper 7, 12–13.

In addition, Petitioner identifies the following proceedings related to the '601 patent: *Croga Innovations Ltd. v. International Business Machines Corporation*, No. 2-23-cv-00634 (E.D. Tex.); *Croga Innovations Ltd. v. Fortinet, Inc.*, No. 2-24-cv-00206 (E.D. Tex.); and *Croga Innovations Ltd. v. Amazon Web Services, Inc.*, No. 1-24-cv-00398 (W.D. Tex.). Pet. 109.

We note that, on September 16, 2024, Palo Alto Networks, Inc. filed a petition for *inter partes* review of the '601 patent based on prior art not asserted in this proceeding. *See Palo Alto Networks, Inc., v. Croga Innovations Ltd.*, IPR2024-01421, Paper 2, 2–3. An institution decision has not been issued in IPR2024-01421 and that proceeding remains pending.

C. The '601 Patent (Ex. 1001)

The '601 patent is titled “Network Isolation for Collaboration Software.” Ex. 1001, code (54). The '601 patent discloses methods and systems “for isolation of multi-user interactive software (e.g., collaboration software) on a host computer system,” which may include a workspace and an isolated computing environment. *Id.* at 1:58–65. Examples of collaboration software include “screen sharing applications, collaborative meeting applications, remote desktop applications, gaming applications, shared document application, file sharing applications, and/or the like,” such as “WebEx, GoToMeeting, etc.” *Id.* at 4:45–47, 4:56–60.

According to the '601 patent, “[o]ne or more applications may run in the workspace via a first memory space (e.g., a trusted memory space),” and “[t]he isolated computing environment may be isolated from the workspace

by an internal isolation firewall.” Ex. 1001, 1:62–67. The ’601 patent further describes that “[o]ne or more isolated applications may run in the isolated computing environment via a second memory space,” wherein “[t]he isolated applications may have access to one or more Internet destinations (e.g., untrusted Internet destinations)” and “communicate with the Internet destinations via an authentication device.” *Id.* at 2:8–13. The ’601 patent also describes a host-based firewall, which “may be configured to isolate the host computer system from communicating with one or more devices on the network.” *Id.* at 2:44–47.

The ’601 patent describes that the isolated applications may include a multi-user interactive software application, which “may be an application that allows one or more remote machines to control (e.g., access, view, interact with, download from, upload to, and/or modify) an application running on the host computer system.” Ex. 1001, 2:18–23. For example, “the multi-user interactive software application may allow the remote machines to view a display of the host computer system (e.g., for a presentation or screen-sharing).” *Id.* at 2:23–26.

According to the ’601 patent, “[i]solation of collaboration software may protect the host computer system from collaboration software-based interactions that may bypass other network security controls.” *Id.* at 4:12–15. The ’601 patent describes systems and methods for providing:

a layer of communication isolation between collaboration software applications and untrusted network destinations in order to prevent malware from effectively exfiltrating data from the host computer system and/or establishing command and control channels with an attacker resources in order to attempt to gain control of the host computer system.

Id. at 4:36–42. Specifically, the '601 patent describes “a sandbox protected application or process and/or an internal isolation firewall running” on the host computer system. *Id.* at 4:61–65. For example, “collaboration software may wholly or partially be contained in a sandboxed computing environment (e.g., an isolated computing environment).” *Id.* at 4:65–5:1.

Figure 2, reproduced below, illustrates a “host computer system configured to participate in a software based meeting with one or more other host computer systems,” wherein the host computer system uses “a sandbox based network isolation system.” Ex. 1001, 3:61–65.

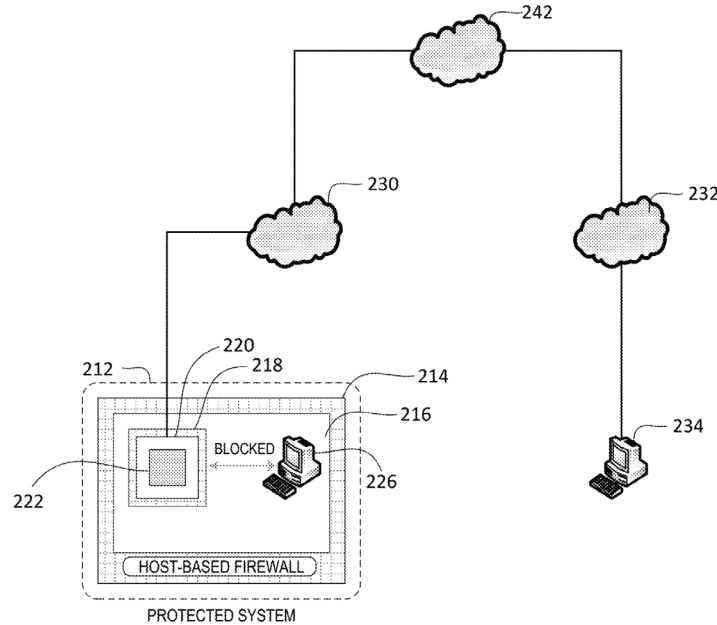


FIG. 2

Figure 2 depicts the host computer system 212 including “a host-based firewall 214, an operating system 226, a sandboxed computing environment (e.g., an isolated computing environment) 220, an internal isolation firewall

218, and a workspace 216.” *Id.* at 9:66–10:3. The host computer system 212 is configured to “isolate communication with untrusted network destinations using one or more of the host-based firewall 214, a border firewall (not shown), a web proxy (not shown), an internal isolation firewall 218, or a segregation of untrusted memory space.” *Id.* at 10:27–31. “The sandboxed computing environment 220 may be enforced via the sandbox container process,” which “may be a security mechanism used to separate resources associated with the sandboxed computing environment 220 from other applications and/or processes that may be running on the workspace 216 of the host computer system 212.” *Id.* at 10:34–40.

The ’601 patent describes that “host computer system 234 may be configured to interact with the host computer system 212 via the collaboration software application (e.g., multi-user interactive software application) 222,” wherein “[t]he host computer system 212 may allow the host computer system 234 to access the sandboxed computing environment 220.” Ex. 1001, 12:4–7, 12:16–18. According to the ’601 patent,

[o]perating the collaboration software application 222 within the sandboxed computing environment 220 may restrict command and control between the host computing system 212 and the untrusted device to the sandboxed computing environment 220 and/or the untrusted memory space of the host computing device 212.

Id. at 11:65–12:3. The ’601 patent explains that

[i]f malware is transferred to the host computer system 212 due to interactions with the host computer system 234, the malware may be isolated to the sandboxed computing environment 220, which may make it difficult for the malware to infect the workspace 216 of the host computer system 212 and/or other devices on the network 230.

Id. at 12:25–30.

D. Challenged Claims

Petitioner challenges claims 1–16 (all) of the '601 patent. Pet. 9. Of the challenged claims, claims 1 and 9 are independent claims. Ex. 1001, 22:42–63; 23:33–24:8. Claim 1 recites:

1. A system comprising:

a memory; and

a processor configured to:

implement a workspace that uses a host operating system, wherein the workspace enables operation of a first set of one or more applications or processes via a first memory space;

implement an isolated computing environment that uses the host operating system, wherein the isolated computing environment enables operation of a second set of one or more applications or processes via a second memory space, and wherein the second set of one or more applications or processes comprises a multi-user interactive software application;

isolate the isolated computing environment from the workspace using an internal isolation firewall;

authenticate the isolated computing environment with an authentication device; and

send data to an untrusted destination from the multi-user interactive software application via a proxy device when the isolated computing environment has been authenticated.

Ex. 1001, 22:42–63.

E. The Asserted Grounds

Petitioner challenges claims 1–16 of the '601 patent based on the grounds set forth in the table below.

Claims Challenged	35 U.S.C. §	Reference(s)/Basis ³
1–4, 7, 9–12, 15	103 ⁴	Jeffries ⁵ , LaBine ⁶ , Ishaya ⁷
5, 6, 13, 14	103	Jeffries, LaBine, Ishaya, Cucinotta ⁸
8, 16	103	Jeffries, LaBine, Ishaya, Levy ⁹

Pet. 20.

Petitioner supports its showing of unpatentability of the challenged claims of the '601 patent with the Declaration of Prashant Shenoy, Ph.D. (Ex. 1003). Patent Owner has not filed a declaration or otherwise challenged the testimony of Dr. Shenoy. Accordingly, at this stage of this proceeding, the testimony of Dr. Shenoy in support of Petitioner's contentions is unrebutted.

³ Petitioner contends that the cited art qualifies as prior art under applicable law. *See* Pet. 20. Patent Owner does not dispute the prior art status of the cited art. *See* Prelim. Resp. We preliminarily determine that the cited art qualifies as prior art.

⁴ The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) ("AIA"), amended 35 U.S.C. § 103, and was effective on March 16, 2013. The application for the '601 patent is U.S. Application No. 16/141,535, filed on September 25, 2018, which claims priority to a provisional application filed on September 28, 2017. Ex. 1001, codes (21), (22), (60), 1:7–9. Because the application for the '601 patent claims a priority date after the effective date of the applicable AIA amendment, the AIA version of § 103 applies for purposes of institution.

⁵ US 10,885,189 B2, issued Jan. 5, 2021, filed May 22, 2017 (Ex. 1005).

⁶ US 2009/0292999 A1, published Nov. 26, 2009 (Ex. 1006).

⁷ US 2014/0282889 A1, published Sept. 18, 2014 (Ex. 1007).

⁸ US 2016/0048406 A1, published Feb. 18, 2016 (Ex. 1008).

⁹ US 2007/0136579 A1, published June 14, 2007 (Ex. 1009).

II. OBVIOUSNESS ANALYSIS

A. Principles of Law

Under 35 U.S.C. § 103, “[a] patent claim is unpatentable if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.” *See KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007) (similar language). The question of obviousness involves resolving underlying factual determinations including (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and when presented (4) objective evidence of non-obviousness (not presented here). *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). Further, “there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.” *See KSR*, 550 U.S. at 418.

B. Level of Ordinary Skill in the Art

Petitioner contends that

A Person of Ordinary Skill in the Art (“POSITA”) in September 2017 would have been someone knowledgeable and familiar with network security and application isolation techniques as those are applied in the context of network security available in the 2010s. That person would have a bachelor’s degree in computer science, computer engineering, electrical engineering, or equivalent training, and approximately two years of experience working in the field of network security.

Pet. 14. Petitioner further contends that “[a]dditional work experience can substitute for educational background, and vice versa.” *Id.* (citing Ex. 1003

¶¶ 20–22). At least at this stage of this proceeding, Patent Owner does not address the level of ordinary skill in the art. *See generally* Prelim. Resp.

Determining the level of ordinary skill in the art involves various factors, including the “type of problems encountered in the art; prior art solutions to those problems; rapidity with which innovations are made; sophistication of the technology; and educational level of active workers in the field.” *In re GPAC Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995) (citation omitted). The prior art of record also reflects the level of ordinary skill in the art. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001). For purposes of this Institution Decision, we adopt the assessment offered by Petitioner, as it is not disputed by the Patent Owner and is consistent with the ’601 patent and the asserted prior art.¹⁰

C. Claim Construction

In *inter partes* reviews, the Board construes claims using the same claim construction standard employed in a civil action under 35 U.S.C. § 282(b). 37 C.F.R. § 42.100(b) (2023). The “words of a claim ‘are generally given their ordinary and customary meaning,’” as would have been understood by a person of ordinary skill in the art at the time of the invention. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc) (quoting *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996)). “In determining the meaning of the disputed claim limitation, we look principally to the intrinsic evidence of record, examining the claim language itself, the written description, and the prosecution

¹⁰ No matter how designated in this Decision, any determination (except our decision to institute trial) is preliminary and non-binding. We wish to have the full record as developed during trial before rendering any binding determination, finding, or conclusion.

history, if in evidence.” *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 469 F.3d 1005, 1014 (Fed. Cir. 2006) (citing *Phillips*, 415 F.3d at 1312–1317).

Petitioner asserts that “for the purposes of this proceeding and the grounds presented herein, no claim term requires express construction.” Pet. 15. At least at this stage of this proceeding, Patent Owner does not address claim construction. *See generally* Prelim. Resp.

Accordingly, at this stage, no need exists to expressly construe any claim terms to resolve the parties’ disputes.¹¹ *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (“[W]e need only construe terms ‘that are in controversy, and only to the extent necessary to resolve the controversy.’” (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))).

D. Asserted Obviousness of Claims 1–4, 7, 9–12, and 15 Based on Jeffries, LaBine, and Ishaya

Petitioner challenges claims 1–4, 7, 9–12, and 15 as being obvious over Jeffries, LaBine, and Ishaya. *See* Pet. 20, 21–91. We start with a description of the disclosures of Jeffries, LaBine, and Ishaya, and then consider the arguments and evidence presented by Petitioner. Patent Owner does not dispute any aspect of the showing in the Petition as to unpatentability of any challenged claim. *See generally* Prelim. Resp.

¹¹ If either party contends that explicit claim construction is necessary in order to make a final determination whether or not any challenged claim is unpatentable based on the arguments and evidence presented, it should clearly explain why during trial and provide a clear and unambiguous construction with supporting evidence including specifically identifying the challenges, claims, and limitations to which the construction is necessary.

1. Jeffries (Ex. 1005)

Jeffries is titled “Isolated Container Event Monitoring.” Ex. 1005, code (54). Jeffries relates to a host operating system “monitor[ing] resource access by an application running in a container that is isolated from the host operating system.” *Id.* at code (57). As background, Jeffries notes that “[c]omputing devices are frequently exposed to attacks from malicious software that can compromise functionality of information stored on the computing devices as well as the devices themselves.” *Id.* at 1:6–9.

According to Jeffries,

[i]n contrast to many virtual machine-based or sandbox approaches, using containers in conjunction with the event monitoring techniques described herein protects the computing device from attacks by isolating web browsers, related applications, and operating system components such as the kernel, the file system, and the network from untrusted resources.”

Ex. 1005, 2:42–49. Accordingly, Jeffries describes that “when the host device requests access to a resource, the host device contains the resource within one or more containers that provide full kernel isolation from the host operating system.” *Id.* at 2:52–55. Jeffries explains that

[w]hen an application accesses a resource in a container, a container event manager implemented in the container monitors container activity that occurs from accessing the resource. The container event manager is configured to generate a security event in response to detecting malicious activity within the container occurring from resource access. In accordance with one or more embodiments, the host operating system considers every resource to be untrusted and forces resources to be accessed within an isolated container. Thus, the container event manager is configured to treat all container activity as malicious activity and constantly generate security events that describe container activity as it occurs in real-time.

Id. at 3:42–54. “The host operating system is configured to determine a threat level associated with each received security event.” *Id.* at 4:62–63. If the “threat level of malicious activity described by a received security event satisfies a threat level threshold, the host operating system takes corrective action to mitigate a negative effect of the malicious activity,” such as “quarantin[ing] the container to prevent the container from accessing any resources or data outside the container.” *Id.* at 5:47–54.

Figure 1 of Jeffries, reproduced below, illustrates an exemplary system implementing isolated container event monitoring. Ex. 1005, 2:17–19.

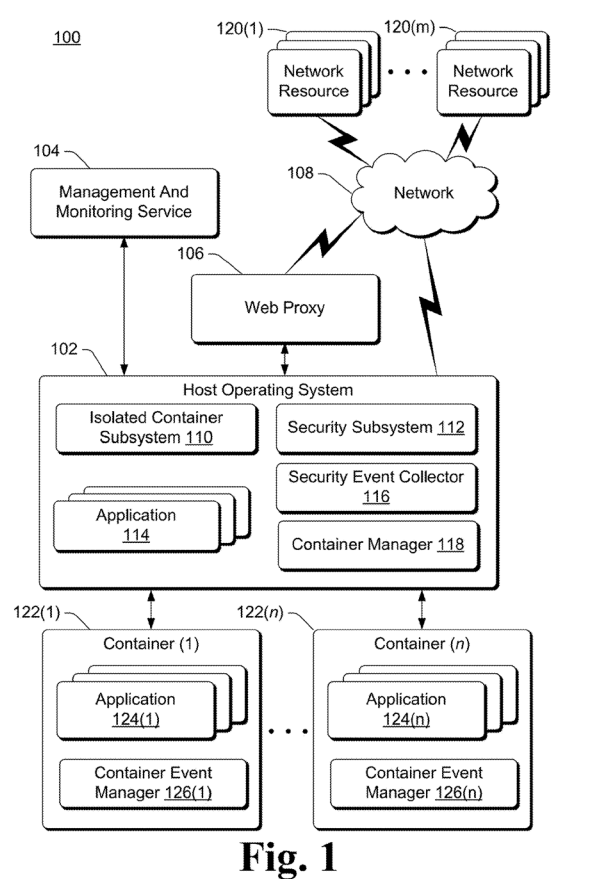


Fig. 1

Figure 1 depicts a system 100 including a host operating system 102, a management and monitoring service 104, and a web proxy 106. *Id.* at 6:44–

46. The host operating system 102 includes “an isolated container subsystem 110, a security subsystem 112, one or more applications 114, a security event collector 116, and a container manager 118,” and “manages one or more containers, illustrated as multiple (n) containers 122(1), . . . , 122(n).” *Id.* at 8:55–60. According to Jeffries,

the security subsystem 112 can receive security events from the security event collector 116 that describe container activity resulting from resource access in one or more of containers 122(1), . . . , 122(n). The security subsystem 112 compares a received security event against policy, such as policy received from management and monitoring service 104, to determine a threat level of the potentially malicious activity. For example, the security subsystem 112 can compare security event information describing the potentially malicious activity against a list of acceptable and/or unacceptable container behavior to determine whether a threat level associated with the malicious activity satisfies a threat level threshold.

Id. at 9:12–24.

Jeffries further describes that “each container event manager 126(1), . . . , 126(n) is configured to monitor activity that occurs when one or more applications 124(1), . . . , 124(n) access a resource within a respective container” and “generate a security event in response to detecting malicious activity within a container 122(1), . . . , 122(n).” Ex. 1005, 11:1–8.

According to Jeffries,

a determination of whether potentially malicious activity indicated by the security event satisfies a threat level threshold is used by the container manager 118 to either allow an application 124(1), . . . , 124(n) to continue accessing resources or take corrective action to mitigate the malicious activity.

Id. at 11:17–23.

2. *LaBine (Ex. 1006)*

LaBine is titled “Desktop Sharing Method and System.” Ex. 1006, code (54). LaBine relates to “a method and system for enabling remote control of a host computer having a display region that is to be shared with at least one other computer.” *Id.* ¶ 1.

Figure 1 of LaBine, reproduced below, illustrates a network topology in which LaBine’s technology is used. Ex. 1006 ¶ 20.

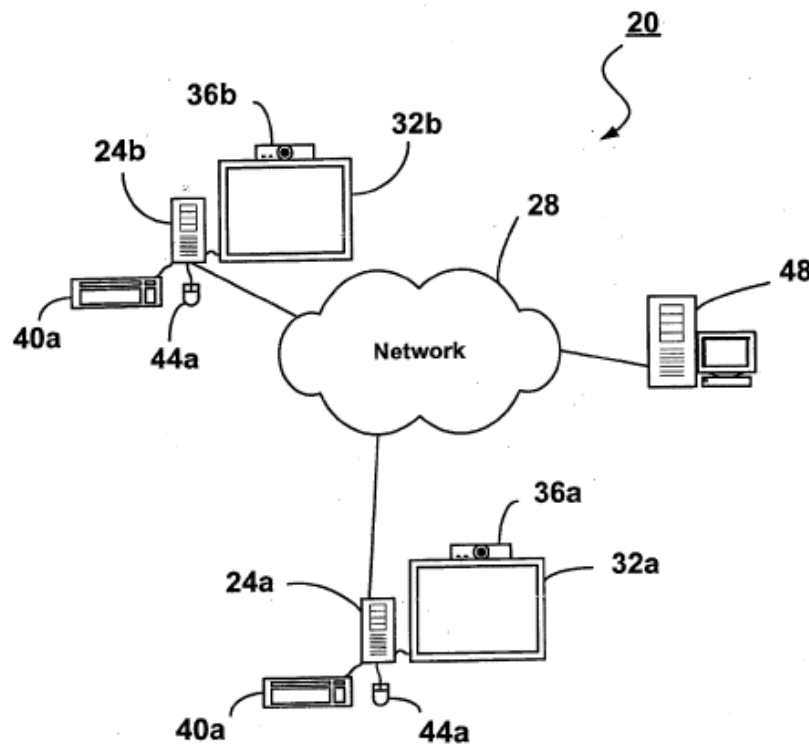


Fig. 1

Figure 1 depicts a computing environment 20 that includes a pair of computers 24a, 24b communicating with touch screens 32a, 32b; web cameras 36a, 36b; keyboards 40a, 40b; and mice 44a, 44b, over a communication network 28. *Id.* ¶ 43. Figure 1 also shows that each of the computers 24a, 24b is also in communication with a conferencing server 48

via the communication network 28. *Id.* LaBine describes that each personal computer 24a, 24b runs a desktop sharing application, such as SMART Bridgit Conferencing Software, that permits the personal computers to share displayed information. *Id.* ¶ 45. According to LaBine,

[t]his desktop sharing application allows a conference to be set up between personal computers with one personal computer at a time being designated as a host, or “presenter” computer and the remaining personal computers being designated as client, or “participant” computers. Images of the host computer desktop are transmitted to the client computers in the conference via the conferencing server 48 and are displayed on the monitors of the client computers full screen. In the environment of FIG. 1, the host computer desktop is presented on the touch screens 32a and 32b.

Id.

LaBine also describes enabling remote control of a host computer. Ex. 1006 ¶ 74. According to LaBine, “[w]here a viewer on a client computer has been given remote control access to the host computer, the viewer can interact with the shared region of the presenter’s desktop on the host computer.” *Id.* LaBine describes that “the conferencing server 48 has been listening for a REMOTE CONTROL request from client computers, which is transmitted when a user clicks with his/her mouse on the shared display region of a client computer.” *Id.* ¶ 78. According to LaBine, once the request is granted, “remote user input events on the client computer having remote control, such as mouse, keyboard and pen input events, are received at the conferencing server 48 from the remote controller and routed to the host computer,” which “treats the remote user input events as though they were input locally.” *Id.* ¶ 84.

3. *Ishaya (Ex. 1007)*

Ishaya is titled “Method and System for Identity-Based Authentication of Virtual Machines.” Ex. 1007, code (54). Ishaya relates to “using identity information for authentication of virtual machines.” *Id.* ¶ 1.

Figure 2 of Ishaya, reproduced below, illustrates an information processing system. Ex. 1007 ¶ 11.

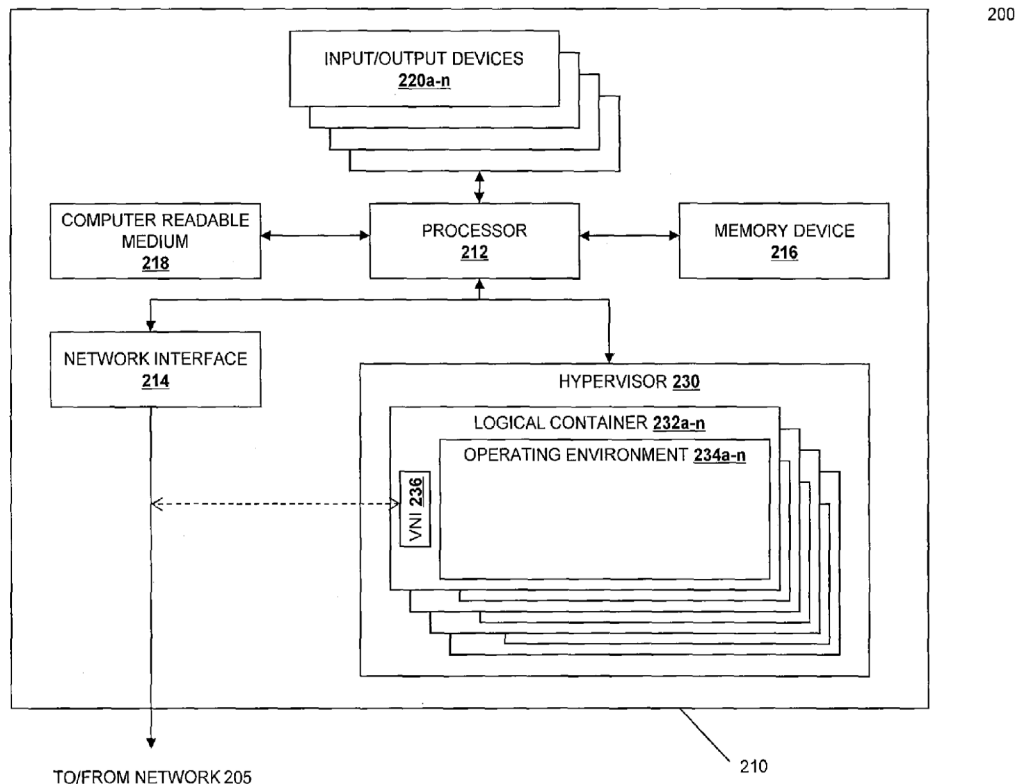


FIGURE 2

Figure 2 shows “an information processing system 210 configured to host one or more virtual machines, coupled to a network 205.” *Id.* ¶ 35. The information processing system 210 includes a hypervisor 230, which may be implemented in software. *Id.* ¶ 40. According to Ishaya, “[t]he hypervisor 230 includes the functionality to add, remove, and modify a number of logical containers 232a-n associated with the hypervisor.” *Id.* ¶ 41. Ishaya

describes that each virtual machine “includes identification data,” which “can include the Media Access Control (MAC) address, the Internet Protocol (IP) address, and one or more unambiguous names or identifiers.” *Id.* ¶ 43.

Figure 7 of Ishaya, reproduced below, illustrates the process of instantiating, launching and authenticating a virtual machine instance. Ex. 1007 ¶ 19.

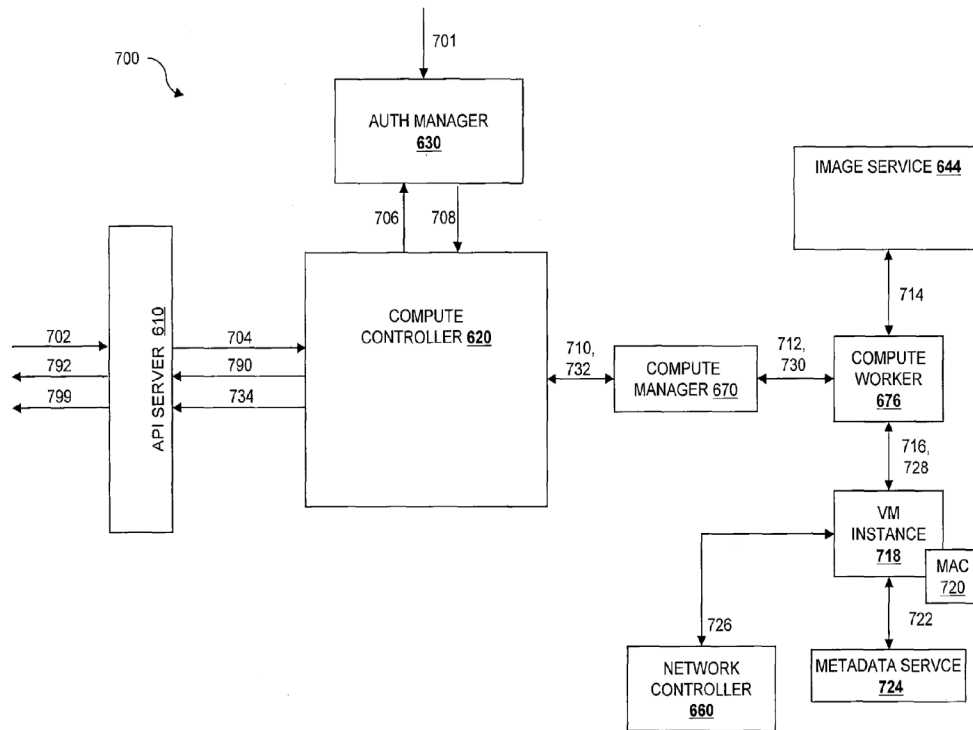


FIGURE 7

Figure 7 depicts an “embodiment of the process of instantiating, launching and authenticating a VM instance is shown as diagram 700.” *Id.* ¶ 174.

Ishaya describes that, “at time 716, the Compute Worker assigns the VM instance 718 a MAC address 720 (or link-local address).” *Id.* ¶ 181. Ishaya also describes another embodiment where “the MAC address 720 is replaced with another immutable value that can be used to convey the identity of VM instance 718,” such as “an IP address, an IP port, a signature value, a unique

identifier,” or “a hash value computed from the VM image used to instantiate the VM instance 718, such as, for example, an SHA-1, SHA-2, or SHA-3 hash.” *Id.*

Ishaya describes that “[a]t time 722, the newly instantiated VM instance 718 begins the process of obtaining its initial configuration by interacting with Metadata Service 724 and Network Controller 660.” Ex. 1007 ¶ 183. According to Ishaya, “the VM instance 718 authenticates to the Metadata Service 724 via an identity as described above.” *Id.* ¶ 184. Ishaya also describes that “[a]t time 726, VM instance 718 interacts with Network Controller 660 to get a proper VLAN and IP address,” wherein “[t]he VM instance 718 again provides its MAC address 720 in order to authenticate itself to the Network Controller 660 and obtain the VLAN and IP address.” *Id.* ¶ 185.

4. Analysis of Independent Claims 1 and 9

For the reasons that follow, we are persuaded that Petitioner establishes sufficiently for the purpose of this institution decision that the subject matter of independent claims 1 and 9 would have been obvious in view of the combination of Jeffries, LaBine, and Ishaya. Our analysis of the showing in the Petition for claims 1 and 9 is provided below.

a. Motivation to Combine the Teachings of Jeffries, LaBine, and Ishaya

Petitioner articulates with supporting reasoning and evidence why a skilled artisan would have been motivated to combine the relevant teachings of Jeffries and LaBine with a reasonable expectation of success. *See* Pet. 28–32 (citing Ex. 1003 ¶¶ 62–73; Ex. 1005, code (57), 2:42–49, 3:48–51, 5:51–54, 9:26–33, 10:54–63, 12:17–22, 15:26–30, 16:37–42; Ex. 1006, code (57), ¶¶ 4, 45, 46, 50, 78–84; Ex. 1036 ¶ 4). With regard to motivation to combine the teachings of Jeffries and LaBine, the Petition provides:

A POSITA would have combined Jeffries with LaBine because both improve the security of a host computer when accessing untrusted resources. . . .

A POSITA would have been motivated to combine Jeffries and LaBine to execute a web conferencing application, like LaBine's, within an isolated container, as described by Jeffries. Doing so would isolate the host computer from any malicious code potentially introduced through the web conferencing application. . . .

A POSITA would have understood that Jeffries' application-isolation techniques were applicable to **any** type of application, including a web conferencing application such as LaBine's. . . .

[A] POSITA would have recognized that a user applying LaBine's web conferencing application would readily benefit from Jeffries' methods of isolating applications in containers. . . .

LaBine's web conferencing is the type of application Jeffries anticipates as being executed within its isolated containers 122. . . .

Combining LaBine with Jeffries would have been a simple combination of prior art elements according to known methods to yield predictable results. In the combination, LaBine's web conferencing application would be isolated within a container as described in Jeffries. . . . This combination would have been predictable with an expectation of success because Jeffries describes isolating any type of application. . . .

In addition, multiple advantages would motivate a POSITA to combine Jeffries with LaBine. The combination advantageously improves the security of a computer system that allows remote control by participating computers. A POSITA would have recognized that a web conferencing application, such as LaBine's, would allow users to collaborate with team members within an organization. With the added layer of

security provided by Jeffries' isolated containers, users could use these same collaborative techniques with unknown participants including sharing files, presenting media content, or granting remote access to users outside of their organization, while protecting the host computer. . . .

A POSITA would have had a reasonable expectation of success in making the combination. While Jeffries' techniques apply to any kind of application . . . , Jeffries specifically contemplates isolating applications that access untrusted resources LaBine's web conferencing application is this type of application because it allows remote access by untrusted users. . . . In addition, Jeffries' container isolation policies are flexible enough to ensure that any application has access to the necessary resources for execution. . . . Running LaBine's web conferencing application in Jeffries' isolated containers would have been within the skillset of a POSITA. . . .

For all these reasons, a POSITA would be motivated to implement a multiuser interactive software application, like LaBine's software, in an isolated container, as described by Jeffries.

Id. We determine that Petitioner establishes motivation to combine the relevant teachings of Jeffries and LaBine.

Petitioner articulates with supporting reasoning and evidence why a skilled artisan would have been motivated to combine the relevant teachings of Jeffries, LaBine, and Ishaya with a reasonable expectation of success. *See* Pet. 32–36 (citing Ex. 1003 ¶¶ 74–91; Ex. 1005, code (57), 2:39–60, 6:44–57, 10:22–53, 14:47–54, 15:14–16, 16:11–31, Fig. 1; Ex. 1007, code (57), ¶¶ 1, 41–43, 174–187, 189–196, Fig. 8; Ex. 1012, 2 (Abstract); Ex. 1013, code (57); Ex. 1014 ¶ 76; Ex. 1015 ¶ 11; Ex. 1018 ¶ 3; Ex. 1019 ¶ 18; Ex. 1020 ¶ 180; Ex. 1037 ¶¶ 4, 66). With regard to motivation to combine the teachings of Jeffries, LaBine, and Ishaya, the Petition provides:

A POSITA would have further combined Jeffries and LaBine with Ishaya because both Jeffries and Ishaya describe improving computer security by isolating containers. . . .

The combination of Jeffries, LaBine, and Ishaya would include implementing the container authentication technique described in Ishaya in the combined Jeffries-LaBine system, such as within the management and monitoring service 104. . . .

Jeffries generally describes the importance of authentication. . . . However, Jeffries combined with LaBine provides limited details regarding the identity of newly created containers or when the container is permitted to communicate after creation. . . .

Ishaya provides these implementation details. Given Jeffries' limited details regarding container creation, a POSITA seeking to implement an isolated container as described by Jeffries would have found it obvious to consult Ishaya. Ishaya describes authenticating a container as part of this process by assigning it a MAC and/or IP address. . . . Ishaya further explains multiple advantages of its container creation process including authentication (e.g., ensuring that the container can be trusted . . .), the ability to authenticate with controllers of other vendors . . . , as well as other advantages. . . .

[T]he combination of Jeffries and LaBine further with Ishaya simply represents combining prior art elements according to known methods to yield predictable results. In the combination, a newly created isolated container, such as a container 122 described in Jeffries . . . , is authenticated as described by Ishaya The results of the combination would have been predictable because Ishaya explains how this process of container isolation improves security with identity-based authentication as an improvement to simple user authentication with usernames and passwords. . . .

In addition, a POSITA would have had a reasonable expectation of success of combining Jeffries and Labine with

Ishaya. A POSITA would have sufficiently understood creating, isolating, and authenticating virtual machines and containers because these concepts were well known at the time. . . . A POSITA would have expected to successfully combine Jeffries and Labine with Ishaya because both Jeffries and Ishaya involve isolating containers and virtual machines. . . .

For these reasons, a POSITA would have implemented the technique of authenticating containers, as taught by Ishaya, in Jeffries’ system. Further, a container in Jeffries would include a video conferencing application, as described by LaBine. Doing so would predictably improve the security of the host computer through identity-based authentication as described by Ishaya.

Id. We determine that Petitioner establishes motivation to combine the relevant teachings of Jeffries, LaBine, and Ishaya.

b. Independent Claim 1

Our limitation-by-limitation analysis of the showing in the Petition for claim 1 is provided below.

*A system comprising:*¹²

Petitioner relies on the disclosure in Jeffries of a system. Pet. 36–37 (citing Ex. 1003 ¶¶ 92–94; Ex. 1005, 6:20–22, Fig. 1). Figure 1 of Jeffries, reproduced above, “illustrates an example system 100 implementing isolated container event monitoring.” Ex. 1005, 6:20–22.

a memory;

Petitioner relies on the disclosure in Jeffries of a memory. Pet. 37–39 (citing Ex. 1003 ¶¶ 95–99; Ex. 1005, 6:37–43, 22:39–42, 23:8–10, Fig. 6).

¹² Petitioner does not discuss whether the preamble of claim 1 is limiting. We determine that the preamble of claim 1 is not limiting because it does not recite essential structure and is not necessary to give life, meaning, and vitality to the claim. *See Shoes by Firebug LLC v. Stride Rite Children’s Group, LLC*, 962 F.3d 1362, 1367 (Fed. Cir. 2020).

Jeffries provides that “the computing device implementing system 100 may range from a full resource device with substantial **memory** and processor resources (e.g., personal computers, game consoles) to a low-resource device with limited **memory** and/or processing resources (e.g., traditional set-top boxes, hand-held game consoles).” Ex. 1005, 6:37–43 (emphasis added).

a processor configured to:

Petitioner relies on the disclosure in Jeffries of a processor. Pet. 40–41 (citing Ex. 1003 ¶¶ 100–103; Ex. 1005, 22:47–50, 22:60–64, Fig. 6). Jeffries provides that, “[t]he example computing device **602** as illustrated [in Figure 6] includes a **processing** system 604” and “the **processing** system **604** is illustrated as including hardware elements **610** that may be configured as **processors**.” Ex. 1005, 22:47–48, 22:62–64 (emphasis added).

*implement a workspace that uses a host operating system,
wherein the workspace enables operation of a first set of one or
more applications or processes via a first memory space;*

Petitioner relies on Jeffries for teaching or suggesting all the elements of this limitation. Pet. 42–50 (citing Ex. 1003 ¶¶ 104–123; Ex. 1005, 1:9–11, 6:44–46, 9:28–33, 12:7–22, Fig. 1). The Petition states that “Jeffries describes resources that are not isolated within an isolated computing environment. These resources that are not isolated correspond to a ‘workspace.’” *Id.* at 44. The Petition includes an annotated version of Figure 1 of Jeffries, reproduced below, which it contends “illustrates multiple components of the system 100 that are not isolated” and are a workspace that uses a host operating system. *Id.* at 43–44.

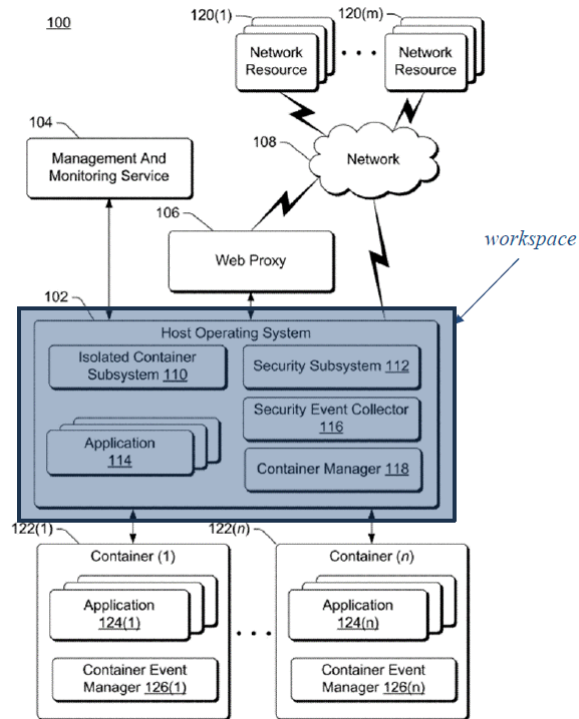


Fig. 1

Id. at 45. Annotated Figure 1 depicts host operating system 102 (highlighted in dark blue), “including the isolated container subsystem 110, applications 114, security subsystem 112, security event collector 116, and container manager 118, [a]s not contained within the isolated computing environments (containers 122) in Jeffries [which] would therefore collectively be a ‘workspace,’ as claimed.” *Id.* at 45–46.

Petitioner also contends that “the ‘memory locations’ supporting the components that are not isolated within isolated containers 122 in Jeffries may correspond to the claimed ‘workspace.’” Pet. 46. In this regard, the Petition provides:

Specifically, Jeffries describes “memory locations associated with the container event manager 126” within isolated containers 122, as contrasted with memory locations associated with “the security event collector 116, the container manager 118, or **any other component of host operating system 102.**” Ex.1005, 12:11-16. The memory associated with the host operating

system 102 is “off-limits” to the “container[s] 122.” Ex.1005, 12:7-22; Ex.1003, ¶¶109-110. Because these “off-limit data or memory locations” are not contained within Jeffries’ isolated computing environments, they may also correspond to a “workspace” as claimed. Ex.1003, ¶¶111-112; *see also* Ex.1005, 1:9-11 (describing “privileged memory locations”).

Id.

Additionally, with regard to this limitation, Petitioner contends that “Jeffries’ resources and memory associated with the host operating system (the ‘workspace’) ‘enables operation of a first set of one or more applications or processes.’” Pet. 47. In support, Petitioner refers to “Jeffries’ applications 114 within the host operating system 102 in Figure 1.” *Id.* With regard to these applications, Jeffries provides:

Applications 114 include one or more applications that are executable by one or more processors of the computing device implementing the host operating system 102. For example, applications 114 may include a web browser application. Alternatively or additionally, applications 114 may include applications such as e-mail applications, word processing applications, spreadsheet applications, visual presentation applications, and the like.

Ex. 1005, 9:26–33.

Further, with regard to this limitation, the Petition states:

Jeffries’ applications 114 are enabled by the workspace “*via a first memory space,*” as claimed. Ex.1003, ¶119.

As explained above, Jeffries describes “memory locations” associated with the host operating system 102. Ex.1005, 12:12-16. Specifically, Jeffries describes “**memory locations associated with**” each component of the host operating system 102, including “the container event manager 126, the security event collector 116, the container manager 118,

or **any other component of host operating system 102.**”
Ex.1005, 12:11-16; Ex.1003, ¶120.

Pet. 49.

implement an isolated computing environment that uses the host operating system, wherein the isolated computing environment enables operation of a second set of one or more applications or processes via a second memory space, and

Petitioner relies on Jeffries for teaching or suggesting all the elements of this limitation. Pet. 50–57 (citing Ex. 1003 ¶¶ 124–145; Ex. 1005, code (57), 2:39–40, 2:52–55, 8:14–17, 8:67–9:15, 9:62–67, 10:25–37, 15:14–30, 17:7–20, 21:4–8, Figs. 1, 5).

The Petition states that Jeffries’ “containers 122(1),..., 122(n)” are “*isolated computing environment[s].*” *Id.* at 50 (alteration in original).

Jeffries states that “when the host device requests access to a resource, the host device contains the resource within one or more containers that provide full kernel isolation from the host operating system.” Ex. 1005, 2:52–55.

Petitioner again relies on an annotated Figure 1, reproduced below.

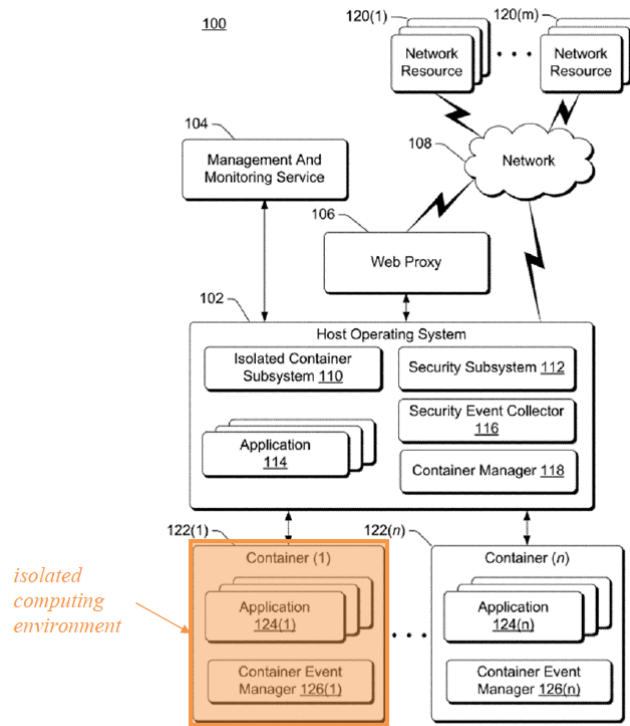


Fig. 1

Id. at 51. This annotated Figure 1 depicts container 122(1) (highlighted in orange) that includes a set of three applications.

The Petition provides that “[i]n Jeffries, processes within an isolated container 122 access **“the shared parts of host operating system 102”** and that “[a]ccessing ‘shared parts of host operating system 102 corresponds to ‘us[ing] the host operating system, as claimed.” Pet. 52 (citing Ex. 1005, 10:25–34). The Petition also states that “Jeffries’s containers 122 rely on several software components in the host operating system 102, including container manager 118.” *Id.* at 53. In this regard, Jeffries provides that “host operating system 102 additionally includes a container manager 118. The container manager 118 manages the scheduling of containers 122(1),..., 122(*n*) in the system 100 and determines which containers 122(1),..., 122(*n*) are run on the host operating system 102 at what times.” Ex. 1005, 9:62–67. Thus, Petitioner establishes that “Jeffries’ containers 122 use the host

operating system for both container monitoring and initial activation and ‘run on the host operating system 102’ while protecting the host operating system 102 from malware through isolation.” *See* Pet. 55.

As noted above, Figure 1 depicts “a set of applications 124(1) running in isolated container 122(1).” *See also id.* The Petition states that “[t]he applications 124 within containers 122 are associated with separate memory space isolated from the memory space of the host operating system 102.” (*id.* at 56) and “[i]n Jeffries, containers 122 are associated with ‘**container memory**’” (*id.* at 57 (citing Ex. 1005, 17:7–20, 21:4–8)).

wherein the second set of one or more applications or processes comprises a multi-user interactive software application;

Petitioner relies on a combination of the teachings of Jeffries and LaBine for this limitation. Pet. 58–63 (citing Ex. 1003 ¶¶ 146–158; Ex. 1005, 9:28–33, 10:54–63; Ex. 1006, code (57), ¶¶ 43, 45, 78–84, Figs. 1, 22–24). With regard to Jeffries and this limitation, the Petition provides:

As described above . . . , Jeffries describes applications 124 in containers 122 that “access untrusted resources[.]” Ex.1005, 10:58-63; Ex.1003, ¶147. Jeffries does not list every type of application 124 that may be executed in the isolated containers 122 in detail. Rather, it provides a non-limiting list of broad categories. *See* Ex.1005, 9:28-33 (“a web browser application,” “email applications, word processing applications, spreadsheet applications, visual presentation applications, and the like”); *see also* Ex.1005, 10:54-58 (applications 124 “correspond to instances of individual ones of the applications 114.”). Jeffries’ techniques of executing applications within isolated containers would have been applied to any type of application. Ex.1003, ¶148.

Pet. 58.

Petitioner relies on LaBine as describing a “multi-user interactive software application.” *Id.* at 58–63. The Petition states that “LaBine describes a video conferencing software that allows participants of the video conference to remotely access and control the host user’s computer” and “LaBine’s software is referred to as the ‘SMART Bridgit Conferencing Software.’” *Id.* at 58. With regard to how this software works, the Petition states:

The “Bridgit Conferencing Software...allows a conference to be set up between personal computers with one personal computer at a time being designated as a host, or ‘presenter’ computer and the remaining personal computers being designated as client, or ‘participant’ computers.” Ex.1006, [0045]. “The client computers can be enabled to control the host computer.” Ex.1006, [0045]; Ex.1003, ¶151.

During a conferencing session, a client computer sends a “REMOTE CONTROL request.” Ex.1006, [0078]. If the “host computer...approves the request,” it sends “a REMOTE CONTROL RESPONSE” which grants the client computer remote control of the host computer. Ex.1006, [0080]-[0081]. With remote control of the host computer, “remote user input events on the client computer..., such as mouse, keyboard and pen events, are received at the conferencing server 48 from the remote controller and routed to the host computer.” Ex.1006, [0084]. The host computer “treats the remote user input events as though they were input locally.” Ex.1006, [0084]; Ex.1003, ¶152.

Pet. 59–60 (alterations in original).

*isolate the isolated computing environment from the workspace
using an internal isolation firewall;*

Petitioner relies on Jeffries as teaching or suggesting this limitation. Pet. 63–65 (citing Ex. 1003 ¶¶ 159–164; Ex. 1005, 12:7–22, 14:40–44, 16:24–46, Fig. 1). Specifically, Petitioner relies on “Jeffries’ container

manager 118, in conjunction with the operating system secure kernel.” *Id.* at 63. The Petition states:

The container manager 118 acts as an “internal isolation firewall” because it “is configured to **quarantine the container 122**” and “**prevents** malicious activity occurring in the container from gaining... **access to shared resources.**” Ex.1005, 16:24-37; *see also id.*, 16:38-46, 14:40-44 (“take corrective action in response to...malicious activity”). The secure kernel (not pictured) helps to enforce the separation between the host operating system 102 and the container 122. *See* Ex.1005, 12:7-22 (“[W]hen malicious software attempts to access off-limit data or memory locations, the secure kernel causes an exception or interrupt to occur.”); Ex.1003, ¶¶160-161.

Id. at 64–65 (alterations in original).

authenticate the isolated computing environment with an authentication device; and

Petitioner relies on teachings in Jeffries and Ishaya for this limitation. Pet. 65–70 (citing Ex. 1003 ¶¶ 165–174; Ex. 1005, 6:53–57, 14:47–52, 14:56–59, 15:9–13, 15:23–26; Ex. 1007 ¶¶ 35, 41, 177–187, 189, 190, 193–196, Figs. 2, 7). The Petition states, with supporting citations to Jeffries and Ishaya, that “Jeffries describes authenticating the host operating system 102 and users of isolated containers 122” and “Ishaya describes authenticating isolated computing environments, referred to as ‘containers.’” *Id.* at 66.

With regard to Jeffries authenticating the host operating system, Jeffries provides that: “web proxy 106 controls access to one or more resources accessed from network 108 by requiring authentication from host operating system 102 before granting access to the one or more resources.” Ex. 1005, 6:54–57. With regard to authenticating users of isolated containers, Jeffries states:

Container manager 118 is responsible for activating one or more containers 122 that are isolated from host operating system 102 to access resources and to take corrective action in response to determining that malicious activity resulting from resource access satisfies a threat level threshold. As discussed herein, activating a container such as container 122 includes creating one or more new containers or resuming running of one or more suspended containers. Container manager 118 is additionally configured to activate one or more containers for an individual user logged into host operating system 102 and ensure that any other users of the host operating system are restricted from accessing the activated one or more containers for the individual user. Container manager 118 ensures a mapping of the user logged into host operating system 102 to the container 122. In some embodiments in which there are multiple users of host operating system 102 and multiple containers, the container manager 118 is configured to see a logged-on user's identity and directly associate that with one or more corresponding containers. This restriction prevents other users from viewing or otherwise interacting with the containers and further prevents the spread of potentially malicious container activity.

Id. at 14:40–62.

With regard to Ishaya authenticating isolated computing environments or containers, the Petition provides:

[T]he containers 232 in Ishaya may be isolated from the remainder of the system. *See* Ex.1007, [0041] (“A corresponding operating environment 234 could enforce separation between users and processes such that each process or group of processes appeared to have sole access to the resources of the operating system.”); Ex.1003, ¶168. . . .

After a container is instantiated, “the Computer Worker assigns the VM instance 718 a MAC address 720” which is “selected from a pool of MAC addresses.” Ex.1007, [0181]. The MAC address may be “replaced with...an IP address.” Ex.1007, [0181]. Then, “[a]t time 722, the newly instantiated VM instance

718...authenticates to the Metadata Service 724 via an identity” such as its MAC address or IP address. Ex.1007, [0183]-[0184]. After this initial authentication, the VM instance receives “possession-based credentials” that it can use “for subsequent authentication to other resources.” Ex.1007, [0184]. For example, at time 726, “[t]he VM instance 718 again provides its MAC address 720 in order to authenticate itself to the Network Controller 660.” Ex.1007, [0185]; Ex.1003, ¶170.

Ishaya describes multiple benefits of authenticating containers. Authenticating an isolated container allows different devices, including other virtual machines or containers to “determine whether or not to trust information from [the container] based on the identity value of” the container. Ex.1007, [0189]. In addition, it increases security even while interoperating with different devices by allowing “controllers from different vendors or entities” to “authenticate to each other.” Ex.1007, [0190]. Ishaya lists multiple other advantages stemming from container authentication. *See also* Ex.1007, [0193]-[0196] (discussing further advantages); Ex.1003, ¶171.

Pet. 67–69 (alterations in original).

send data to an untrusted destination from the multi-user interactive software application via a proxy device when the isolated computing environment has been authenticated.

Petitioner relies on teachings in Jeffries, LaBine, and Ishaya for this limitation. Pet. 70–74 (citing Ex. 1003 ¶¶ 176–182; Ex. 1005, 3:48–51, 6:49–53, 6:64–67, 7:50–54, 10:58–63, Fig. 1; Ex. 1006 ¶¶ 46, 48, 50, 51, 75, Figs. 22, 23; Ex. 1007 ¶¶ 183, 192, Fig. 8). The Petition states that, “[i]n the combined system, a video conferencing application, such as the one described by LaBine, is executed within an isolated container, as described in Jeffries, after the container is authenticated, as described by Ishaya” and “LaBine’s multi-user interactive software . . . *send[s] data to an untrusted destination* because it allows participants of the video conference to share a

view of their computer screen.” *Id.* at 70–71. With further regard to LaBine and its teachings related to this limitation, the Petition provides:

The users of the client computers in Labine may be any user, known or unknown. But regardless of the level of trust of the user of the client computer, LaBine allows “**any** client computer during the conference to be granted remote control of the host computer.” Ex.1006, [0075]. Allowing any client computer to control the host computer would also involve sending data to an untrusted destination. For example, the “REMOTE CONTROL RESPONSE” sent from the host to the client requesting remote control would correspond to data sent to an untrusted destination. *See* Ex.1006, [0046], [0048], [0050]; Ex.1003, ¶177. Similarly, Jeffries’ “applications 124(1),..., 124(n) are thus useable to access **untrusted resources** in one or more of containers 122(1),..., 122(n).” Ex.1005, 10:58-63, 3:48-51; Ex.1003, ¶178.

Id. at 71 (alterations in original).

Petitioner relies on Jeffries for its teachings related to a proxy device.

Pet. 71–73. The Petition provides:

In Jeffries, communication with an untrusted destination occurs via the web proxy 106, which corresponds to “*a proxy device*.” The web proxy 106 is positioned between the host computer (including the host operating system 102 and the isolated containers 122) and external network resources 120, as shown in Figure 1. . . . Ex.1003, ¶179.

The web proxy 106 “controls access to one or more network resources 120(1),..., 120(m).” Ex.1005, 6:49-53. In one embodiment, the network resources 120 represent external network resources, such as “web sites, web applications, emails, [or] documents,” Ex.1005, 6:64-67, that are treated as untrusted resources and “access[ed]... in a container 122(1),..., 122(n),” Ex.1005, 7:50-54; Ex.1003, ¶180.

Id. (second, third, and fourth alterations in original).

Based on the evidence cited and reasoning provided in the Petition, we determine that Petitioner has established that the combination of Jeffries, LaBine, and Ishaya teaches or suggests all the limitations of claim 1.

c. Independent Claim 9

Independent claim 9 is a method claim and independent claim 1 is a system claim. Ex. 1001, 22:42–63, 23:33–24:8. Otherwise, claims 1 and 9 are substantially similar and contain almost all the same language. *See id.* Petitioner relies on the same evidence and reasoning provided with respect to its challenge to the unpatentability of claim 1 in challenging the patentability of claim 9. *See* Pet. 85–88.

Our determination as to claim 9 follows from our determination as to claim 1. Based on the evidence cited and reasoning provided in the Petition, we determine that Petitioner has established that the combination of Jeffries, LaBine, and Ishaya teaches or suggests all the limitations of claim 9.

d. Summary as to Independent Claims 1 and 9

Petitioner has shown that the combination of Jeffries, LaBine, and Ishaya teaches or suggests all the limitations of claims 1 and 9. Petitioner provides articulated reasoning with rational underpinnings to support combining the relevant teachings of Jeffries, LaBine, and Ishaya. As noted previously, Patent Owner does not dispute any aspect of Petitioner's showing as to unpatentability and does not provide any contrary arguments or evidence. We determine that there is a reasonable likelihood that Petitioner will prevail with respect to the unpatentability of claims 1 and 9.¹³

¹³ Thus, we determine that there is a reasonable likelihood that the Petitioner will prevail with respect to at least one of the claims challenged in the Petition pursuant to 35 U.S.C. § 314 and that *inter partes* review should be instituted. Accordingly, we institute as to all the challenged claims and all

5. *Dependent Claims 2–4, 7, 10–12, and 15*

Petitioner also asserts that dependent claims 2–4, 7, 10–12, and 15 are obvious in view of a combination of the teachings of Jeffries, LaBine, and Ishaya. Pet. 74–85, 88–91. The Petition provides a detailed and supported showing that the additional limitations recited in dependent claims 2–4, 7, 10–12, and 15 are taught by Jeffries, LaBine, and Ishaya. *Id.*

Patent Owner does not address the showing in the Petition as to dependent claims 2–4, 7, 10–12, and 15. *See generally* Prelim. Resp.

We determine that there is a reasonable likelihood that Petitioner will prevail with respect to the unpatentability of claims 2–4, 7, 10–12, and 15.

E. Asserted Obviousness of Dependent Claims 5, 6, 13, and 14 Based on Jeffries, LaBine, Ishaya, and Cucinotta

Petitioner challenges dependent claims 5, 6, 13, and 14 as being obvious over Jeffries, LaBine, Ishaya, and Cucinotta. *See* Pet. 20, 91–102.

1. *Cucinotta (Ex. 1008)*

Cucinotta is titled “Scheduling.” Ex. 1008, code (54). Cucinotta relates to “a method of adjusting a scheduling parameter associated with a runnable in a multi-programmed computing system, a computer program product and scheduling unit operable to perform that method.” Ex. 1008 ¶ 1. As background, Cucinotta explains that

[t]ypical multi-programmed computing systems, such as those comprising an Operating System (OS) running multiple processes, or a Virtual Machine Monitor (VMM) running multiple virtual machines (VMs), scheduling of runnable entities (“runnables” comprising processes or VMs) is performed by a

the challenges raised in the Petition. 37 C.F.R. §42.108(a) (“When instituting *inter partes* review, the Board will authorize the review to proceed on all of the challenged claims and on all grounds of unpatentability asserted for each claim.”).

scheduler. The scheduler of OS or VMM runtime is typically configured to implement scheduling in accordance with parameters associated with each runnable. When a runnable is waiting for reception of data packets, a scheduling state associated with that runnable is changed from “ready-to-run” to “sleeping” (or suspended). If a packet for a sleeping runnable is received by a scheduler, the runtime is configured to wake the runnable and change its scheduling state from sleeping (or suspended) back to ready-to-run.

Id. ¶ 2.

Figure 1 of Cucinotta, reproduced below, schematically illustrates the “progress of an incoming packet through a typical virtualised computing environment.” Ex. 1008 ¶ 31.

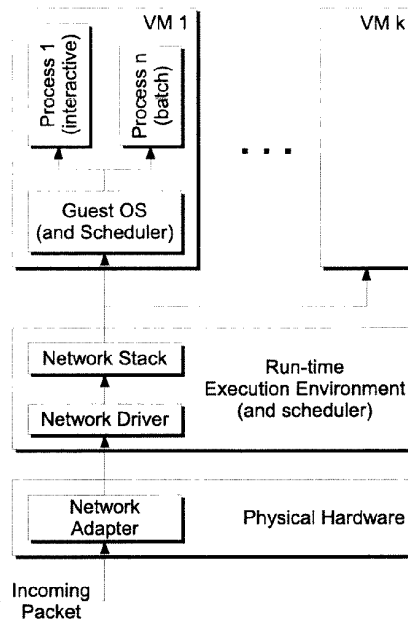


Figure 1: the walk of a network packet being received by a virtualized application, from the physical network adapter through which it is received, to the process within a VM that handles it.

Figure 1 depicts a virtual machine VM1, which is configured to host an interactive network service (e.g., a web server) or a network activity (e.g., a monitoring or logging service or performance of software updates). *Id.* ¶ 32.

According to Cucinotta, “VM1 is associated with a set of scheduling parameters at the VMM scheduler,” wherein the scheduling parameters “may comprise, for example, a priority value or, for deadline-based scheduling, a specific computing deadline.” *Id.*

Cucinotta describes that “a runtime environment, for example, OS or VMM, has a software component which is configured to observe network activity of all runnables, for example, processes or VMs, in the system.” Ex. 1008 ¶ 39. According to Cucinotta, “[t]he software component may comprise a firewall component configured to inspect each and every incoming and outgoing packet.” *Id.* Cucinotta further describes “modifying firewall software, such as the open-source iptables for Linux (<http://en.wikipedia.org/wiki/Iptables>).” *Id.* ¶ 49.

Such firewall software is typically operable to intercept all incoming and outgoing traffic travelling across a computing system, and it can also be used in combination with a KVM hypervisor when using Linux as host OS. In such a realization, iptables operates to intercept any incoming, outgoing, or forwarded traffic travelling across a Linux system, including instances when such traffic is directed towards KVM handling VMs.

Id.

2. *Dependent Claims 5, 6, 13, and 14*

The Petition provides a detailed and supported showing that the additional limitations recited in dependent claims 5, 6, 13, and 14 are taught by Jeffries, LaBine, Ishaya, and Cucinotta. Pet. 95–102. Petitioner articulates with supporting reasoning and evidence why a skilled artisan would have been motivated to combine the relied-on teachings of Jeffries, LaBine, Ishaya, and Cucinotta. *Id.* at 93–95.

Patent Owner does not address the showing in the Petition as to dependent claims 5, 6, 13, and 14. *See generally* Prelim. Resp.

We determine that there is a reasonable likelihood that Petitioner will prevail with respect to the unpatentability of claims 5, 6, 13, and 14.

F. Asserted Obviousness of Dependent Claims 8 and 16 Based on Jeffries, LaBine, Ishaya, and Levy

Petitioner challenges dependent claims 8 and 16 as being obvious over Jeffries, LaBine, Ishaya, and Levy. *See* Pet. 20, 102–108.

1. Levy (Ex. 1009)

Levy is titled “Web Browser Operating System.” Ex. 1009, code (54). Levy discloses “[a] Web browsing system using a browser operating system (BOS)” that “runs the client-side component of each Web application (e.g., on-line banking, and Web mail) in its own virtual machine, which provides strong isolation between Web services and the user’s local resources.” *Id.* at code (57).

Levy describes advantages of the virtual machine environment provided for the browser instance:

First, the Web application is safe from interference by other applications. Second, it is free to modify any machine state, transient or persistent, without endangering other applications or the user's host operating system. Third, the user can easily remove all local effects of a Web application by simply deleting its virtual machine. Finally, the VM environment increases flexibility for the programming of Web applications.

Ex. 1009 ¶ 46.

Levy describes a new browser architecture that

enables users to gain knowledge and control of the active Web content being downloaded and executed and enables Web services to gain the ability to restrict the set of sites with which their applications can communicate, thereby limiting damage

from hijacked browsers. Active Web content and the browser that interprets and renders it are thereby isolated in a private virtual machine, protecting the user’s desktop from side-effects, malicious or otherwise.

Id. ¶ 14; *see also id.* ¶¶ 57 (“The resulting architecture isolates Web applications, protecting other applications and client resources from malicious downloaded code.”), 130 (“In the new browser architecture, each Web application is isolated within its own virtual machine sandbox, removing the need to trust Web browsers and the services they access.”).

2. *Dependent Claims 8 and 16*

The Petition provides a detailed and supported showing that the additional limitations recited in dependent claims 8 and 16 are taught by Jeffries, LaBine, Ishaya, and Levy. Pet. 106–108. Petitioner articulates with supporting reasoning and evidence why a skilled artisan would have been motivated to combine the relied-on teachings of Jeffries, LaBine, Ishaya, and Levy. *Id.* at 103–105.

Patent Owner does not address the showing in the Petition as to dependent claims 8 and 16. *See generally* Prelim. Resp.

We determine that there is a reasonable likelihood that Petitioner will prevail with respect to the unpatentability of claims 8 and 16.

III. DISCRETIONARY INSTITUTION, 35 U.S.C. § 314(A)

Institution of an *inter partes* review is discretionary. *See* 35 U.S.C. § 314(a) (authorizing institution of an *inter partes* review under particular circumstances, but not requiring institution under any circumstances); *Cuozzo Speed Techs., LLC v. Lee*, 579 U.S. 261, 273 (2016) (“[T]he agency’s decision to deny a petition is a matter committed to the Patent Office’s discretion.”); *SAS Inst., Inc. v. Iancu*, 138 S. Ct. 1348, 1356 (2018)

(“[Section] 314(a) invests the Director with discretion on the question whether to institute review” (emphasis omitted)); *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1367 (Fed. Cir. 2016) (“[T]he PTO is permitted, but never compelled, to institute an IPR proceeding.”).

Patent Owner urges the Board to exercise discretion to deny institution of *inter partes* review under § 314(a) based on the factors set forth in *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 at 5–6 (PTAB Mar. 20, 2020) (precedential) (“*Fintiv*”). Prelim. Resp. 1–12. Petitioner contends that discretionary denial would be inappropriate. Pet. 15–19.

An advanced state of a parallel district court proceeding is a “factor that weighs in favor of denying the Petition under § 314(a).” *NHK Spring Co. v. Intri-Plex Techs., Inc.*, IPR2018-00752, Paper 8 at 20 (PTAB Sept. 12, 2018) (precedential) (“*NHK*”). Specifically, an early trial date is part of a “balanced assessment of all relevant circumstances in the case, including the merits.” Consolidated Trial Practice Guide November 2019 (“TPG”) 58.¹⁴

This balanced assessment involves consideration of the following factors:

1. whether the court granted a stay or evidence exists that one may be granted if a proceeding is instituted;
2. proximity of the court’s trial date to the Board’s projected statutory deadline for a final written decision;
3. investment in the parallel proceeding by the court and the parties;
4. overlap between issues raised in the petition and in the parallel proceeding;

¹⁴ Available at <https://www.uspto.gov/TrialPracticeGuideConsolidated>.

5. whether the petitioner and the defendant in the parallel proceeding are the same party; and

6. other circumstances that impact the Board's exercise of discretion, including the merits.

Fintiv, Paper 11 at 5–6.

On June 21, 2022, the Director of the United States Patent and Trademark Office issued a Memorandum setting forth an “Interim Procedure for Discretionary Denials in AIA Post Grant Proceedings with Parallel District Court Litigation” (“Guidance Memo”),¹⁵ providing additional guidance on the application of *Fintiv*. The application of this guidance is further guided by the precedential decisions of the Director in *OpenSky Indus., LLC v. VLSI Tech. LLC*, IPR2021-01064, Paper 102, 49–50 (PTAB Oct. 4, 2022) (precedential) and *CommScope Techs. LLC v. Dali Wireless, Inc.*, IPR2022-01242, Paper 23 (PTAB Feb. 27, 2023) (precedential) (“*CommScope*”). Accordingly, if we determine that the first five *Fintiv* factors favor discretionary denial, we are instructed to consider whether the merits determined under the sixth *Fintiv* factor are compelling. *CommScope*, 4–5. “Compelling, meritorious challenges are those in which the evidence, if unrebutted in trial, would plainly lead to a conclusion that one or more claims are unpatentable by a preponderance of the evidence.” Guidance Memo 4. We make the determination as to whether to exercise our discretion to deny institution consistent with the Guidance Memo.

Our analysis of the *Fintiv* factors is provided below.

¹⁵ Available at https://www.uspto.gov/sites/default/files/documents/interim_proc_discretionary_denials_aia_parallel_district_court_litigation_memo_20220621_.pdf

Factor 1: whether the court granted a stay or evidence exists that one may be granted if a proceeding is instituted

There is no stay in the district court. *See* Pet. 15; Prelim. Resp. 4. As of the time the parties filed the Petition and the Preliminary Response, no motion requesting a stay of the district court proceedings had been filed by either party. *Id.* Petitioner contends that “the Board should not infer the outcome of such a motion” and “this factor is neutral on discretionary denial.” Pet. 15–16. Patent Owner contends “it is unlikely that a stay would be granted in the district court” (Prelim. Resp. 4) and “[t]his factor weighs against institution” (*id.* at 6).

Our independent review of the docket in the district court action indicates that a motion for a stay has been filed but not ruled upon. However, we do not think that we should speculate as to whether a stay may be granted if this proceeding is instituted.

We determine that this factor is neutral.

Factor 2: proximity of the court’s trial date to the Board’s projected statutory deadline for a final written decision

Trial is set to begin in the district court on October 25, 2025. Pet. 16 n.1; Prelim. Resp. 6; Ex. 1031, 1. The projected deadline for the final written decision in this proceeding is February, 2026. Petitioner argues that, “[g]iven the proximity of the Board’s expected Final Written Decision and the estimated trial date, this factor is at least neutral.” Pet. 16. Patent Owner contends that “[t]his factor weighs against institution.”

The Guidance Memo instructs that “when other relevant factors weigh against exercising discretion to deny institution or are neutral, the proximity to trial should not alone outweigh all those other factors.” Guidance Memo 8. The Guidance Memo also instructs that “[p]arties may present evidence

regarding the most recent statistics on median time-to-trial for civil actions in the district court.” *Id.* The parties present such statistics (Ex. 1032, 35) and agree that the projected trial date based on these statistics is late December, 2025. Pet. 16; Prelim. Resp. 7.

We determine that the trial date in the district court (whether based on the set trial date or median time-to-trial statistics) is reasonably proximate to the projected statutory deadline for a final written decision. We are likely to be making our decision at about the same time as a decision will be rendered in the district court.

We determine that this factor weighs marginally in favor of not exercising our delegated discretion to deny institution.

Factor 3: investment in the parallel proceeding by the court and the parties

“This investment factor is related to the trial date factor, in that more work completed by the parties and court in the parallel proceeding tends to support the arguments that the parallel proceeding is more advanced, a stay may be less likely, and instituting would lead to duplicative costs.” *Fintiv*, Paper 11 at 10. If, at the time of the institution decision, a district court has issued substantive orders related to the challenged patent, such as a claim construction order, this circumstance weighs in favor of denial. *See id.* at 9–10. On the other hand, if the district court has not issued such orders, this circumstance weighs against discretionary denial. *Id.* at 10. Moreover, in evaluating this factor, “[i]f the evidence shows that the petitioner filed the petition expeditiously, such as promptly after becoming aware of the claims being asserted, this fact has weighed against exercising the authority to deny institution under *NHK*.” *Id.* at 11.

Neither party directs our attention to any substantive orders entered in the district court. Pet. 17; Prelim. Resp. 7–8. Petitioner argues that the parties have made little investment in the parallel proceeding and that it filed the Petition “within weeks of receiving revised infringement contentions (identifying the asserted claims).” Pet. 17. The Petition was filed on August 13, 2024, and the revised infringement contentions were filed on July 16, 2024. Ex. 1038, 2.

We determine this factor favors institution.

Factor 4: overlap between issues raised in the petition and in the parallel proceeding

Petitioner stipulates that “if trial is instituted, it will not pursue the same grounds in the district court litigation.” Pet. 17 (citing *Sand Revolution II, LLC v. Cont’l Intermodal Group-Trucking LLC*, IPR2019-01393, Paper 24 at 12 (PTAB June 16, 2020) (informative)). Patent Owner points out that “Petitioner has not stipulated to not pursue in a parallel district court proceeding the same grounds as in the petition or any grounds that could have reasonably been raised in the petition (*i.e.*, a *Sotera* stipulation).” Prelim. Resp. 9 (citing *Sotera Wireless, Inc. v. Masimo Corp.*, IPR2020-01019, Paper 12 at 18-19 (PTAB Dec. 1, 2020) (precedential as to § II.A)).

The Guidance Memo provides:

If the petition includes the same or substantially the same claims, grounds, arguments, and evidence as presented in the parallel proceeding, this fact has favored denial. [*Fintiv*, Paper 11 at] 12. Conversely, if the petition includes materially different grounds, arguments, and/or evidence than those presented in the district court, this fact has tended to weigh against exercising discretion to deny institution. *Id.* at 12- 13.

Guidance Memo 7. The Guidance Memo instructs that “the PTAB will not deny institution of an IPR or PGR under *Fintiv* . . . where a petitioner stipulates not to pursue in a parallel district court proceeding the same grounds as in the petition or any grounds that could have reasonably been raised in the petition.” *Id.* at 9.

Based on the Petitioner’s stipulation, the same grounds will not be raised in the parallel proceeding. Patent Owner argues that Petitioner has asserted the same prior art against the challenged claims in both the parallel proceeding and this proceeding and that “there is complete overlap with respect to Petitioner’s invalidity arguments and evidence.” Prelim. Resp. 9. However, according to the Docket Control Order, pretrial disclosures (witness list, deposition designations, and exhibit list) are not due in the parallel proceeding until August 4, 2025. Ex. 1031, 3. At this point, it would be speculation as to whether the same or substantially the same claims, grounds, arguments, and evidence will be presented in the district court as in this proceeding. Without speculating, all we can determine is that the same grounds will not be raised in the parallel proceeding and that the same or substantially the same claims, arguments, and evidence may be presented in both proceedings. Thus, the risk of overlap exists.

As in *Sand Revolution*, “Petitioner’s stipulation, however, mitigates to some degree the concerns of duplicative efforts between the district court and the Board, as well as concerns of potentially conflicting decisions.” *Sand Revolution*, IPR2019-01393, Paper 24 at 12. As informed by *Sand Revolution* (*see id.*), we find that this factor weighs marginally in favor of not exercising our delegated discretion to deny institution.

Factor 5: whether the petitioner and the defendant in the parallel proceeding are the same party

There is no dispute that the petitioner and the defendant in the parallel proceeding are the same party. Pet. 18; Prelim. Resp. 10. This factor weighs marginally in favor of exercising our delegated discretion to deny institution.

Factor 6: other circumstances that impact the Board's exercise of discretion, including the merits

The factors typically considered in the exercise of discretion are part of a balanced assessment of all the relevant circumstances in the case, including the merits. *Fintiv*, Paper 11 at 14. For example, if the merits of a ground raised in the petition seem particularly strong on the preliminary record, this fact has favored institution. *Id.* at 14–15. By contrast, if the merits of the grounds raised in the petition are a closer call, then that fact has favored denying institution when other factors favoring denial are present. *Id.* at 15.

Petitioner argues that “[t]he prior art in this Petition presents a compelling case on the merits,” because an element of the independent claims that the Applicant for the ’601 patent argued was not shown by the art before the Office during prosecution is found in Jeffries. Pet. 18. Petitioner also argues that “the remaining limitations were also known and would have been obvious to use in combination” and “[t]he prosecution examiner allowed the claims without evaluating their unpatentability in view of these prior art references.” *Id.* at 18–19. Patent Owner responds that “[e]ven assuming, *arguendo*, that Petitioner is correct with respect to Jeffries, Petitioner still fails to show that the Petition presents a compelling case for all elements of any claim.” Prelim. Resp. 12.

As discussed above, under *CommScope*, we consider whether the merits are compelling only after a determination that the first five *Fintiv* factors favor discretionary denial. Here, factor 1 is neutral, factors 2, 4 and 5 marginally weigh in favor of exercising our delegated discretion, and factor 3 weighs in favor of not exercising our delegated discretion. As a result, the first five factors slightly favor not exercising our delegated discretion to deny institution.

Given that the first five factors only slightly favor not exercising our delegated discretion to deny institution, it is instructive (although not necessary) to explore the sixth factor, which further favors not exercising our delegated discretion to deny institution. Here, Petitioner set forth a detailed showing, supported by expert testimony, demonstrating how the asserted teaches or suggests every claim limitation. On this record, Patent Owner has not identified a single defect in that evidence nor has Patent Owner submitted any argument or evidence rebutting that showing. Thus, on this record, Petitioner's showing is unrebutted. Further, we have not independently found any defects or issues with Petitioner's showing. Thus, the current record would plainly lead to the conclusion that all challenged claims are unpatentable by a preponderance of the evidence. Thus, the sixth factor favors not exercising our delegated discretion to deny institution.

We clarify that our determination that the current record would plainly lead to the conclusion that all challenged claims are unpatentable by a preponderance of the evidence is obviously based on the current record. The record after trial may have additional arguments and evidence that may not plainly lead to the conclusion that all challenged claims are unpatentable by a preponderance of the evidence. Additional arguments and evidence and a

further review by the panel could result in the determination that the Petitioner has not met its burden of proving unpatentability by a preponderance of the evidence for one, some, or all challenged claims.

We determine that the sixth factor favors institution.

Conclusion on Discretionary Denial

Factor 1 is neutral; factors 2, 4 and 5 weigh marginally in favor of denying institution; and factors 3 and 6 weigh in favor of institution. The Board “holistic[ally] view[s] . . . whether efficiency and integrity of the system are best served by denying or instituting review” when evaluating the *Fintiv* factors under § 314(a). *Fintiv*, Paper 11 at 6. Based upon analysis of the *Fintiv* factors and considering the record as a whole, our holistic view is that efficiency and integrity of the system are best served by instituting review.¹⁶ Thus, we do not exercise our discretion to deny institution under Section 314(a).

IV. CONCLUSION

For the foregoing reasons, we determine that trial should be instituted on claims 1–16 of the ’601 patent.

V. ORDER

Upon consideration of the record before us, it is:

ORDERED that, pursuant to 35 U.S.C. § 314(a), an *inter partes* review of claims 1–16 of U.S. Patent No. 11,223,601 B2 is instituted with respect the grounds set forth in the Petition (*see* Pet. 20); and

FURTHER ORDERED that, pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4(b), *inter partes* review of U.S. Patent No. 11,223,601 B2

¹⁶ We would reach the same conclusion if we did not consider factor 6.

IPR2024-01283
Patent 11,223,601 B2

shall commence on the entry date of this Order, and notice is hereby given of the institution of a trial.

IPR2024-01283
Patent 11,223,601 B2

FOR PETITIONER:

Theodore Foster
David McCombs
Eugene Goryunov
Adam Erickson
HAYNES AND BOONE, LLP
ipr.theo.foster@haynesboone.com
david.mccombs.ipr@haynesboone.com
eugene.goryunov.ipr@haynesboone.com
adam.erickson.ipr@haynesboone.com

FOR PATENT OWNER:

Brett Cooper
Seth Lindner
BC LAW GROUP, P.C.
bcooper@bc-lawgroup.com
slindner@bc-lawgroup.com

Robert Auchter
AUCHTER PLLC
robert@auchterlaw.com