IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of:	Blair Nicodemus *et al.*	
U.S. Patent No.:	8,955,038	Attorney Docket No.: 54971-0010IP1
Issue Date:	Feb. 10, 2015	
Appl. Serial No.:	13/587,505	
Filing Date:	Aug. 16, 2012	
Title:	METHODS AND SYSTEMS FOR CONTROLLING ACCESS TO COMPUTING RESOURCES BASED ON KNOWN SECURITY VULNERABILITIES	

Mail Stop Patent Board
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

PETITION FOR *INTER PARTES* REVIEW OF UNITED STATES PATENT NO. 8,955,038 PURSUANT TO 35 U.S.C. §§ 311–319, 37 C.F.R. § 42

TABLE OF CONTENTS

I. INTRODUCTION 1

II. REQUIREMENTS FOR IPR—37 C.F.R. §42.104 1
- **A.** Grounds for Standing Under 37 C.F.R. § 42.104(a) 1
- **B.** Challenge and Relief Requested Under 37 C.F.R. §42.104(b) 1

III. THE '038 PATENT 2
- **A.** Brief Description 2
- **B.** Prosecution History 6
- **C.** Level of Ordinary Skill 7
- **D.** Claim Construction 8

IV. THE CHALLENGED CLAIMS ARE UNPATENTABLE 9
- **A.** [GROUND 1] – CLAIMS 1, 23, 25, 31, 33 WOULD HAVE BEEN OBVIOUS OVER COUILLARD AND FREUND 10
  1. Couillard (EX1004) 10
  2. Freund (EX1005) 12
  3. Motivation to combine Couillard and Freund 15
  4. The combination of Couillard and Freund renders the Challenged Claims obvious 18
     - (i) Claim 1 18
     - (ii) Claim 23 44
     - (iii) Claim 25 47
     - (iv) Claim 31 49
     - (v) Claim 33 51

V. PTAB DISCRETION SHOULD NOT PRECLUDE INSTITUTION 54
- **A.** The *Fintiv* Factors Favor Institution—§314(a) 54
- **B.** § 325(d) Favors Institution 56
- **C.** *General Plastic* Factors Favor Institution—§314(a) 56
  1. Factors 1, 2, 4, and 5: CrowdStrike and PAN Are Entirely Separate Entities 57
  2. Factor 3: Patent Owner's Staggered Litigation Strategy Precipitated the Staggered Filing of the Petitions 58
  3. Factors 6 and 7: The Distinct Grounds and Lack of Significant Relationship Ensure the Board's Resources and Ability to Render a Decision Within the Statutory Timeframe Are Not Significantly Impacted 58

VI. FEES 60

VII. CONCLUSION.....60

VIII. MANDATORY NOTICES UNDER 37 C.F.R § 42.8(a)(1).....60
- **A.** Real Party-In-Interest Under 37 C.F.R. § 42.8(b)(1).....60
- **B.** Related Matters Under 37 C.F.R. § 42.8(b)(2).....60
- **C.** Lead And Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3).....62
- **D.** Service Information 62

EXHIBITS

EX1001	U.S. Patent No. 8,955,038 ("the '038 Patent")
EX1002	Excerpts from the Prosecution History of the '038 Patent ("the Prosecution History")
EX1003	Declaration of Dr. Markus Jakobsson
EX1004	U.S. Patent Appl. Pub. No. 2006/0203815 to Alain Couillard ("Couillard")
EX1005	U.S. Patent No. 5,987,611 to Gregor Freund *et al.* ("Freund")
EX1006	U.S. Patent Appl. Pub. No. 2004/0103220 to Bill Bostick *et al.*
EX1007	U.S. Patent No. 7,415,100 to Robert S. Cooper *et al.*
EX1008	U.S. Patent No. 9,298,474 to Frederic Bauchot *et al.*
EX1009-EX1099	[RESERVED]
EX1100	*In re: Taasera Licensing LLC, Patent Litigation*, Case No. 2:22-md03042, Docket No. 1, "Transfer Order" (EDTX Aug. 3, 2022)
EX1101	*Memorandum: Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation* (June 21, 2022) ("Director's Memo")
EX1102	*In re: Taasera Licensing LLC, Patent Litigation*, Case No. 2:22-md03042, Docket No. 278, "Eighth Amended Docket Control Order" (EDTX Sep. 7, 2023)

CLAIM LISTING

Limitation	Claim Language
1[pre]	A method for controlling the operation of an endpoint, comprising:
1[a]	providing a user interface, at a computing system remote from the end point, configured to allow configuration of a plurality of policies;
1[b]	maintaining the plurality of policies in a data store on the computing system;
1[c]	identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to monitor;
1[d]	configuring one or more software agents on the endpoint to monitor the plurality of operating conditions;
1[e]	receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the one or more software agents;
1[f]	determining, by the computing system, a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store; and
1[g]	initiating, by the computing system, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by a processor on the endpoint.
23[pre]	A system for controlling the operation of an endpoint, comprising:
23[a]	a user interface, provided by a computing system remote from the end point, configured to allow configuration of a plurality of policies;
23[b]	a data store, at the computing system, that contains the plurality of policies;
23[c]	one or more software agents on the endpoint configured to monitor a plurality of operating conditions identified in the plurality of policies; and
23[d]	one or more hardware processors at the computing system configured to:

Limitation	Claim Language
23[d.i]	receive, across a network, status information about the plurality of operating conditions on the endpoint gathered by the one or more software agents,
23[d.ii]	determine a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store, and
23[d.iii]	initiate, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by the hardware processor on the endpoint.
[25]	The system of claim 23, wherein the user interface comprises a web page.
[31]	The system of claim 23, wherein the conditions comprise at least one software condition.
[33]	The system of claim 23, wherein the plurality of policies includes at least one policy that includes the at least one rule that identifies the action.

I. INTRODUCTION

CrowdStrike, Inc. ("CrowdStrike" or "Petitioner") petitions for *Inter Partes* Review ("IPR") of claims 1, 23, 25, 31, 33 ("the Challenged Claims") of U.S. Patent No. 8,955,038 ("the '038 Patent"). CrowdStrike respectfully submits that an IPR should be instituted, and that the Challenged Claims should be canceled as unpatentable.

II. REQUIREMENTS FOR IPR—37 C.F.R. §42.104

A. Grounds for Standing Under 37 C.F.R. § 42.104(a)

CrowdStrike certifies that the '038 Patent is available for IPR. The present petition is being filed within one year of service of a complaint against CrowdStrike. CrowdStrike is not barred or estopped from requesting this review of the Challenged Claims.

B. Challenge and Relief Requested Under 37 C.F.R. §42.104(b)

Petitioner requests IPR of the Challenged Claims on the grounds identified below.

Ground	Claims	Basis for Rejection
1	1, 23, 25, 31, 33	Obvious (§103) over Couillard and Freund

The application that issued as the '038 Patent was filed on August 16, 2012, and claims priority to a provisional application filed on December 21, 2005. EX1001, cover. While Petitioner does not concede that December 21, 2005 (i.e.,

the "Critical Date") is the priority date that should be accorded to the '038 Patent, for the purposes of this proceeding, each of the references asserted in this Petition qualifies as prior art even if the filing date of the provisional application is used as the priority date of the '038 Patent.

Reference	Date	Section
Couillard	Filed 03/10/2005	102(e)
Freund	Issued 11/16/1999	102(b)

III. THE '038 PATENT

A. Brief Description

The '038 Patent describes "methods and systems for flexibly monitoring, evaluating, and initiating actions to enforce security compliance policies." EX1001, 6:36-38. FIG. 2 of the '038 Patent (reproduced below) illustrates process 200 for "controlling the access of endpoint system 104 to host system 102." EX1001, 8:65-9:17.

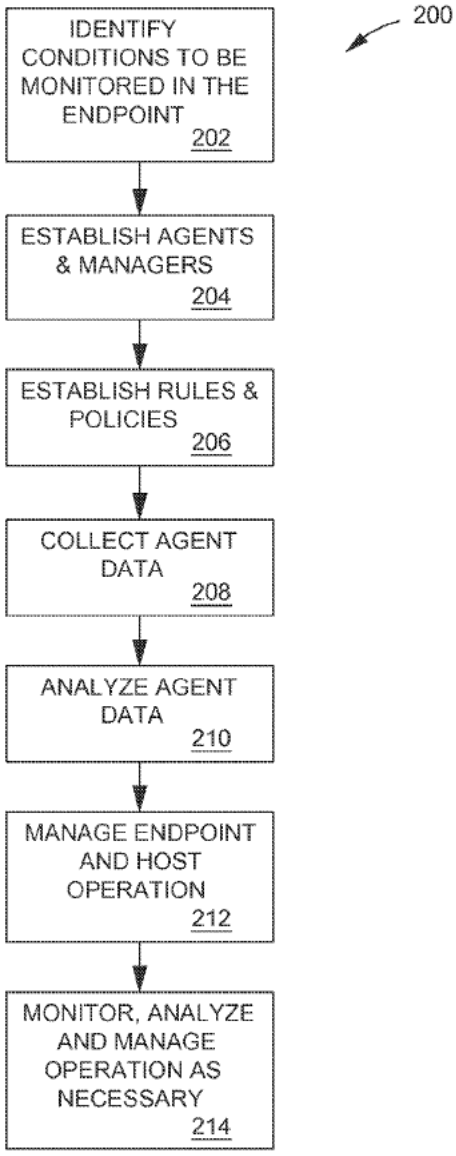


FIG. 2

Initially, "conditions" are identified for the system to monitor. EX1001, 9:28-33. The '038 Patent describes these "conditions" broadly, noting that "there are many different data sources and data elements that can be examined to assess the state of the endpoint, form compliance assessments, and ultimately make pol-

icy-based access control decisions regarding local and remote computing resources." *Id.* The '038 Patent includes a long list of "illustrative conditions," which include, for example, "Installed service packs," "Running applications," "Antivirus scanning state (e.g. active, idle)," and "Date of last software update." *See* EX1001, 10:21-14:52.

"Subsequent to identifying the various conditions to be monitored within endpoint system 104 (step 202), the various agents 104E and agent managers 104D and agent monitor(s) 104C are identified and configured for monitoring those various conditions (step 204)." EX1001, 14:54-57. "Agents can be free standing external software applications, system services provided by the operating system or dedicated, special-purpose monitoring processes that are part of the monitored system itself." EX1001, 15:1-4. In one example, "an agent manager 104D may be configured to query a vendor specific API exposed by a third party antivirus agent, may be configured to query an operating system service periodically to determine if the endpoint has an active network interface and if so, the IP address of that interface, etc." EX1001, 14:57-62.

Next, "there are . . . established rules and policies for controlling the access to local resources on the endpoint system 104 or remote host system 102 (step 206)." EX1001, 15:30-36. "The policies established to control access to host system 102 and/or access to local host resources 102G . . . , can specify a number of

behavioral options for endpoint system 104." EX1001, 15:37-40. "[C]onfiguration policies include both the configurable behaviors of the compliance analysis engine and the security policies of the systems," including, for example, "[s]ampling interval," an "[e]numerated list of compliance thresholds for different endpoint data elements," "[p]assword expiration age or date," and "[r]equired operating system patches to run a specific application." *See* EX1001, 15:44-21:5.

Next, "the various condition data described above is collected by the agent managers through the agents (step 208) and then analyzed (step 210)." EX1001, 24:34-36. "The analysis engine analytical model compares current condition information 104F, policies regarding those conditions 106B and makes action decisions resulting from those conditions and policies, using one or more analytical models." EX1001, 26:29-32. The analysis engine 106C "initiates actions to permit, deny or control access to local and/or remote computing resources based on additional policies that identified permitted and/or denied actions when a noncompliance condition exists." EX1001, 26:33-37.

"[W]hen policy violations are detected it may be desired to take one or more discrete actions to either bring the endpoint into compliance, prevent harm from coming to the local and/or remote computers, restrict user actions, or perform any number of different actions (step 212)." EX1001, 50:47-52. "Policy actions may be endpoint actions allowed to take place because the endpoint system 104 is in

compliance with security policies, actions to take to partially or wholly restrict access to endpoint resources because the endpoint system 104 is not in compliance with security policies, or a combination thereof." EX1001, 51:4-9. Examples of endpoint policy actions include "[i]nitiate password reset," "[d]elete a malicious file," and/or "[p]ermit or deny network access to an enumerated list of IP addresses or IP network numbers." *See* EX1001, 51:30-53:20, 53:37-54:18. This "process of managing the endpoint and host operations repeats as frequently as necessary (step 214)." EX1001, 50:58-60.

B. Prosecution History

The '038 Patent issued from U.S. Patent App. No. 13/587,505 (the '505 application). The claims of the '505 application were rejected for under 35 U.S.C. § 101, and several claims were rejected as anticipated by U.S. Pat. Pub.2005/0086511 (Balacheff) or rendered obvious by Balacheff in view of U.S. Patent No. 7,805,752 (Newstadt) or U.S. Pub. No 2077/0124803 (Taraz). *See* EX1002, 110-124. To overcome the § 101 rejection, the Applicant amended one independent claim to recite that the claimed "action" is "carried out by a processor on the endpoint," and noted that another independent claim recited "one or more processors at the computing system configured to . . . ." *See* EX1002, 96-101. To overcome the prior art rejections, the Applicant argued that Belecheff did not de-

scribe or suggest "identifying, from the plurality of policies, a plurality of conditions on the endpoint to monitor," "configuring one or more software agents on the endpoint to monitor the plurality of conditions," or that "the action is carried out by a processor on the endpoint." *See* EX1002, 101-103.

In allowing the claims, the Examiner entered an Examiner's Amendment in which the term "conditions" was changed to "operating conditions" in several instances, and the processors were specified to be "hardware processors." EX1002, 67-69. Furthermore, the Examiner indicated that Balacheff "teaches providing a user interface, at a computing system remote from the end point, configured to allow configuration of a plurality of policies; [and] maintaining the plurality of policies in a data store on the computing system." *See* EX1002, 69. However, the Examiner did not believe that the prior art of which he was aware taught or suggested the combination of the remaining "identifying," "configuring," "receiving," "determining," and "initiating" limitations of the independent claims. *See id.* at 69-70. However, the Examiner did not consider the Couillard reference relied upon in this petition, which alone and/or in combination with Freund teaches and suggests these limitations.

C. Level of Ordinary Skill

A person of ordinary skill in the art relating to the subject matter of the '038 Patent as of December 21, 2005 ("POSITA") would have possessed a bachelor's

degree in computer science, computer engineering, or an equivalent, as well as two years of industry experience and would have had a working knowledge of endpoint monitoring systems and software security analysis. EX1003, ¶26. Greater education or greater experience could compensate for a deficiency in either of these criteria. EX1003, ¶26.

D. Claim Construction

All claim terms should be construed according to the *Phillips* standard. *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005); 37 C.F.R. § 42.100. In co-pending litigation, certain parties proposed construing certain claims terms:

Claim Term	Plaintiff's Construction	Opposing[1] Construction
"compliance state of the endpoint"	Plain meaning	Level of compliance by the endpoint with compliance policy thresholds
"compliance policies"	Plain meaning	The items on an endpoint to monitor, the analysis methods to use, and the

[1] These constructions were proposed by other defendants in the co-pending litigation and were not affirmatively advocated by Petitioner or a real party-in-interest.

		permitted thresholds for the monitored items

Here, because the Challenged Claims are obvious under all of these constructions, or any reasonable construction, no express constructions are required in this proceeding because "claim terms need only be construed to the extent necessary to resolve the controversy." *Wellman, Inc. v. Eastman Chem. Co.*, 642 F.3d 1355, 1361 (Fed. Cir. 2011).

To be clear, Petitioner reserves the right to address any construction proposed by Patent Owner or the Board. Petitioner also reserves the right to pursue constructions in district court that are necessary to decide matters of infringement. Furthermore, CrowdStrike is not conceding that each challenged feature satisfies all statutory requirements such as 35 U.S.C. §112. As this is an IPR petition, CrowdStrike is pursuing prior art-based grounds. CrowdStrike is not waiving any arguments concerning other grounds that can only be raised in district court.

IV. THE CHALLENGED CLAIMS ARE UNPATENTABLE

The prior art described below demonstrates each of the features that the Examiner noted during prosecution.

A. [GROUND 1] – CLAIMS 1, 23, 25, 31, 33 WOULD HAVE BEEN OBVIOUS OVER COUILLARD AND FREUND

1. Couillard (EX1004)

Couillard "relates to verification of compliance of a device connecting to a corporate network (for example a Local Area Network (LAN)) . . . and connection of the device according to a result of the compliance verification." EX1004, [0002]. The system described by Couillard "protects existing corporate networks by only giving access to compliant workstations and by keeping vulnerable systems out." EX1004, [0015]. "Non-compliant desktops and laptops can be automatically warned and/or quarantined until remediation." *Id.*

Couillard's system comprises "'Compliancy Appliance Server' (CAS) deployed centrally within the corporate network along with a lightweight Compliancy Security Agent (CSA) software installed on the workstations." EX1004, [0040]. "The CAS operates as soon as a workstation plugs itself into any network port and a boot up of the device is detected 85." EX1004, [0045]. "At this point, the CAS transparently isolates 87, 88 the workstation within a 'Compliancy VLAN' (external to corporate resources) and performs 89, 90, 91, 92 a compliancy scan within a few milliseconds." *Id.* "Based on the result of this scan 93, the workstation is then redirected either to its adequate 'Production VLAN' (if deemed compliant) 95 or, alternatively, it may be redirected to either a 'Restricted VLAN' with access to limited resources and where repairs and patch uploads may take

place, or a 'Quarantine VLAN' to quarantine the workstation 94." *Id.* "All of these actions are performed based on the compliancy scanning results and depend on the security policies programmed in the CAS by the corporate network administrators and security analysts." *Id.*

Couillard's system allows an organization to define a set of Corporate Compliancy Rules (CCR), which are "compliancy process[es] through which is checked a state of the device." *See* EX1004, [0048], [0064]. "The state can be the presence or absence of any information on the device." EX1004, [0064]. For example, the CCRs may include "information concerning all the OS patches, the Antivirus, the spyware, the versions of any piece of software, etc." EX1004, [0064]. The "CSA verifies the compliance of each rule in the set of rules transmitted by the CAS." *See generally* EX1004, [0129]-[0156]. "[A]s soon as a required rule is not complied with by a device, the device is deemed non-compliant." EX1004, [0061]. "Corrections are made to the device and the process is repeated until the device is deemed compliant." *Id.* "The corrections (remediation) can be made manually or automatically depending on the network settings." *Id.*

Couillard describes the CSA as "lightweight . . . software installed on the workstations." EX1004, [0040]. FIG. 3 illustrates the CSA as including various functional components, such as a compliance verifier 72 that "obtain[s] the compliance verification results." EX1004, [0043]. However, beyond these and similarly

high-level functional descriptions, Couillard does not dictate or otherwise limit the exact form that the CSA takes, such as the implementation details of the compliance verifier 72 or how it "obtain[s] the compliance verification results." *See id.*; EX1003, ¶59. Thus, a POSITA would have naturally turned to other prior art and their own knowledge to provide these implementation details. EX1003, ¶59.

2. Freund (EX1005)

Freund relates to "system and methods for regulating access and maintaining security of individual computer systems and local area networks (LANs) connected to larger open networks (Wide Area Networks or WANs), including the Internet.." EX1005, 1:25-30. Like Couillard, Freund recognizes the security risks from more corporate computers and networks being connected to the Internet, including "attacks by perpetrators (hackers) capable of damaging the local computer systems, misuse these systems, or steal proprietary data and programs." *See* EX1005, 1:58-2:14; EX1003, ¶60.

To account for these security risks, Freund describes system and methods providing network administrators, workgroup supervisor[s], and individual PC users with the ability to monitor and regulate the kinds of exchanges permissible between one's local computing environment and external network or WANs, including the Internet." EX1005, 3:41-46; EX1003, ¶61. More specifically, the system "provides a client-side filter that is controlled by the centralized authority as long

as the centralized authority has a way of enforcing non-compliance, for example, by blocking access to an open network, such as a WAN or the Internet." EX1005, 3:55-59.

Like Couillard, Freund's system includes two main structural components: "a client-based filter application (installed at each client), and a central supervisor application that maintains the access rules for the client based filter and verifies the existence and proper operation of the client-based filter application." EX1005, FIG. 3A, 12:45-65, 14:52-15:11; EX1004, FIG. 3, [0040]; EX1003, ¶62. "The client-based filter application, which in a preferred embodiment performs all of the monitoring, logging, and filtering work, is responsible for intercepting process loading and unloading," as well as "keeping a list of currently active processes; . . . [and] intercepting and interpreting all TCP/IP communication and build[ing] a comprehensive representation of these TCP/IP activities." EX1005, 13:23-33. The supervisor application, which is typically installed on a server computer that can be reached via a network by all monitored workstations, "monitors whether a client has the filter application loaded and provides the filter application with the rules for the specific user or workstation." EX1005, 13:66-14:5.

In its "Overview" section, Freund also describes an "access management application [that] is employed by the LAN administrator, workgroup administrator,

and/or LAN user to maintain a database of the access rules for the workstations being administrated." EX1005, 12:66-13:22. However, Freund does not again refer to the access management application. EX1003, ¶63. While Freund does not explicitly describe where the access management application would be executed/hosted, a POSITA would have understood or at least found it obvious that in at least some of the embodiments disclosed in Freund, the access management application would be executed/hosted on the same server as the centralized supervisor application. EX1003, ¶63. For example, Freund describes that the supervisor application "specifies rules which govern Internet access by the client computers including the particular client computer" and "provides the filter application with the rules for the specific user or workstation." EX1005, 5:38-41, 13:66-14:5. Thus, even though Freund does not explicitly describe that the access management application and centralized supervisor application are executed/hosted on the same server, a POSITA would have understood or at least found it obvious that it would be particularly efficient to host the component that "specifies" and "provides" the rules (i.e., the centralized supervisor application) on the same server or server system that "maintain a database of the access rules" (i.e., the access management application). *See generally* EX1005, 12:45-14:12; EX1003, ¶63.

To perform the "monitoring, logging, and filtering work," the client-based filter application includes a data acquisition module 440, which is illustrated and

described with respect to FIGS. 4 and 5. *See* EX1005, 15:12-16:29, 20:50-21:46; EX1003, ¶64. The data acquisition module 440, which is preferably implemented as a Windows VxD driver, includes several "hooks" that allow the data acquisition module 440 to hook into various operating system components. EX1005, 20:50-63. For example, data acquisition module 440 includes a "File Hook 503" that "includes functionality allowing the driver 440 to hook into the file subsystem provided by the underlying operating system." EX1005, 20:54-57. Similarly, "Process Hook 505" is a subcomponent that "hooks into the underlying operating system, [and] tracks all currently-executing applications or processes." EX1005, 20:57-60. Each of these hooks "are capable of executing at ring 0--that is, execution at the highest privileged level of the operating system." EX1005, 20:60-63.

3. Motivation to combine Couillard and Freund

Both Couillard and Freund are analogous art in the same field of art as the '038 Patent, which is at least as broad as controlling endpoint access to computing resources based on the evaluation and enforcement of a set of rules. *See* EX1001, Abstract; EX1004, Abstract; EX1005, Abstract; EX1003, ¶65. Given these similarities and based on at least the above noted teachings and their own knowledge, a POSITA would have found it obvious to look to the teachings of Freund when implementing certain features of Couillard's system. EX1003, ¶65.

In a first example, a POSITA would have recognized that Freund provides teachings of at least one obvious way to implement Couillard's CSA to "obtain the compliance verification results." EX1004, [0043]; EX1003, ¶66. As described above, Freund teaches that client-based filter application includes a data acquisition module 440 that includes several "hooks" that allow the data acquisition module 440 to hook into various operating system components and facilitate the "monitoring, logging, and filtering work" performed by the client-based filter application. *See* EX1005, 15:12-16:29, 20:50-21:46; EX1003, ¶66. "By intercepting process loading and unloading and keeping a list of currently active processes, each client process can be checked for various characteristics, including checking executable names, version numbers, executable file checksums, version header details, configuration settings, and the like." EX1005, 13:34-39. Similarly, "[b]y intercepting certain file activity and assigning them to the originating process, the system can track files being created and changed by any process in order to match TCP/IP activities with corresponding file activities." EX1005, 13:57-60.

Like Freund's client-based filter application, Couillard describes that its CSA determines the state for the device with respect to rules transmitted by the CAS, where the rules may include the presence, absence, or status of various information of the mobile device, including "any set up and configuration" data.

EX1004, [0129]-[0156]; EX1003, ¶67. While Couillard does not dictate or otherwise limit how the CSA collects this compliancy information, a POSITA would have found it obvious to look to Freund (e.g., the various hooks utilized by Freund's client-based filter application) to provide at least one obvious implementation of an element of the CSA for collecting at least a portion of the compliancy information. EX1003, ¶67. As explained by Freund, hooking into operating system components (e.g., the Winsock communication driver and/or file subsystem) was at least one known way to detect security features or attributes (e.g., checking configuration settings for currently active applications) used to evaluate compliance with security policies. *See* EX1005, 13:23-65, 15:12-16:7, 20:50-63; EX1003, ¶67. A POSITA would have been motivated to utilize Freund's teachings, for example, because Freund teaches that these hooks execute "at ring 0," which offers them the highest privilege level and therefore access to the greatest amount of relevant and secure information. *See* EX1005, 20:60-63; EX1003, ¶67. Further, a POSITA would have recognized that Couillard and Freund monitor overlapping conditions (e.g., both monitor the list of running processes), and therefore would have naturally turned to Freund for implementation details on how to monitor these conditions. *See* EX1004, [0144]-[0155]; EX1005, 13:23-65, 20:50-63; EX1003, ¶67.

A POSITA would have had a reasonable expectation of success in implementing this Couillard-Freund combination, because both systems are similarly structured (i.e., a central server maintaining and evaluating rules based on conditions that are monitored by software installed on endpoint/client devices), and the implementation details provided by Freund are intended for use in a similar operating system structure as described in Couillard (e.g., both Couillard and Freund describe the use of Microsoft Windows operating system on the endpoint/client devices). *See* EX1004, [0040], [0142]; EX1005, 5:36-41, 7:13-30; EX1003, ¶68. Furthermore, this was a highly predictable art using well known techniques. EX1003, ¶68. Thus, it would have been well within the skill of a POSITA to implement the Couillard-Freund combination. EX1003, ¶68.

4. The combination of Couillard and Freund renders the Challenged Claims obvious

(i) Claim 1

[1pre]

To the extent the preamble is deemed to be limiting, the Couillard-Freund combination renders it obvious. EX1003, ¶71. Couillard describes a system with two primary elements: a "Compliancy Appliance Server (CAS) deployed centrally within the corporate network along with a lightweight Compliancy Security Agent (CSA) software installed on the workstations." EX1004, [0040]. The CAS and CSAs work together to perform compliancy scans when a workstation attempts to

log onto a corporate network. *See* EX1004, [0045]-[0046]. As soon as a workstation plugs itself into a managed network, the CAS and CSA set up an SSL session during which the CAS transparently isolates the workstation within a "Compliancy VLAN" external to corporate resources and performs a compliancy scan. EX1004, [0045]-[0046]. Only after the workstation is determined to be complaint with the security policies programmed in the CAS by the corporate network administrators and security analysts will it be permitted to access the corporate resources. EX1004, [0045]-[0046]. In this regard, "the CAS . . . provides corporate IT personnel the ability to monitor and ***control*** the entire corporate fleet of ***devices (laptop, desktop, PDA, etc.)*** used by users accessing the network." EX1004, [0051][2]. A POSITA would have understood that Couillard's workstations/devices that include a Compliancy Security Agent (CSA) are "endpoints," as that term is used in the '038 Patent. EX1001, 7:52-59 ("endpoint system 104 comprises any processing system capable of interconnecting with host system 102, for example: a ***laptop computer, personal computer***, server system, enterprise system, ***personal digital assistant***, cellular telephone, smart telephone or other personal device, or ***any other processing system capable of remotely accessing host system 102 for the purpose of accessing the resources available there on***."); EX1003, ¶71.

[2] Emphasis added throughout unless otherwise noted.

[1a]

The Couillard- Freund combination teaches 1[a] or at least renders 1[a] obvious. EX1003, ¶¶72-77. For example, Couillard teaches that the actions of the system "are performed based on the compliancy scanning results and depend on the ***security policies*** programmed ***in the CAS by the corporate network administrators and security analysts***." EX1004, [0045]. Thus, the security policies are programmed into the Compliancy Appliance Server (CAS) side 76. EX1003, ¶72.

With respect to FIG. 2, Couillard teaches that its "invention is composed of a OSI Layer-2 Network Appliance, the 'Compliancy Appliance Server' (CAS) ***deployed centrally within the corporate network*** along with a lightweight Compliancy Security Agent (CSA) software installed on the workstations." EX1004, [0040]. The CSAs on the workstations communicate with the central CAS via TCP/IP connection. *See* EX1004, [0041]. Couillard further teaches that the "term 'corporate network' is intended to cover a Local Area Network (LAN), a Metropolitan Area Network (MAN) and a Wide Area Network (WAN)." EX1004, [0018]. Accordingly, at least where the corporate network encompasses a MAN or WAN—networks in which components are often separated into remote geographic locations—a POSITA would have understood or at least found it obvious that the Compliancy Appliance Server (CAS) side 76 into which the security policies are programmed is remote from at least some of the workstations/client devices that

include the Compliancy Security Agents (CSAs). *See* EX1004, FIG. 3, [0018]; *see also* [0051] (explaining that "the entire corporate fleet of devices" includes mobile devices such as laptops and PDAs that would have been able to connect wirelessly via WAN); EX1003, ¶73.

Couillard teaches that the "system is preferably accessible within an ***administrator management interface***, such as the Microsoft-based Management Console (MMC), which network and system administrators are already familiar with and use on a daily basis to monitor, manage and query desktops, laptops, servers, networks and other LAN resources." EX1004, [0053]. As noted above, Couillard teaches that "the security policies [are] programmed ***in the CAS***," so a POSITA would have understood or at least found it obvious that the CAS would include the administrator management interface through which at least some of those policies (e.g., rules) are programmed. EX1004, [0045]. Furthermore, it was well known in the art to specify security policies through a central server. EX1003, ¶74.

For example, as described in Section, IV.A.2, *supra*, Freund describes an "access management application [that] is employed by the LAN administrator, workgroup administrator, and/or LAN user to maintain a database of the access rules for the workstations being administrated." EX1005, 12:66-13:22. And with respect to FIGS. 7A-K, Freund "illustrate[s] a preferred user interface or 'wizard'

dialogs for configuring rules." EX1005, 24:16-17. Freund does not explicitly describe where the access management application and/or rule wizard interface would be executed/hosted.[3] EX1003, ¶75. However, Freund describes that the supervisor application—which is hosted on the server accessed by the client workstations—"specifies rules which govern Internet access by the client computers including the particular client computer" and "provides the filter application with the rules for the specific user or workstation." EX1005, 5:38-41, 13:66-14:5. Thus, even though Freund does not explicitly state that the access management application and centralized supervisor application are executed/hosted on the same server, a POSITA would have understood or at least found it obvious that it would be practical and efficient to host the component that "specifies" and "provides" the rules (i.e., the centralized supervisor application) on the same server or server system that "maintain[s] a database of the access rules" (i.e., the access management application). *See generally* EX1005, 12:45-14:12; EX1003, ¶75.

[3] This contrasts with the separate user interface illustrated in FIGS. 6A-E, which Freund describes specifically as provided by the client-side monitoring component, and would therefore be executed on the client workstations on which the client-side monitoring component is installed. EX1005, 12:54-61, 22:44-47; EX1003, p. 44, n. 2.

Indeed, because Freund does not separately specify a server or other device for the access management application and/or rule wizard interface in the Internet-based (client/server) system 300 illustrated in FIG. 3A, there are only a finite and limited number of provided devices on which to execute/host the access management application and/or rule wizard interface. *See* EX1005, 14:52-15:11. A POSITA thus would have found at least the server 321, which also executes/hosts the supervisor component 323, to have been a logical host for the access management application and/or rule wizard interface for at least the reasons noted above. EX1003, ¶76. When applied in the context of Couillard's system, a POSITA would have understood Freund's similar teachings to describe or at least suggest that Couillard's administrator management interface through which the system's security policies are configured would be executed/hosted at the central server that also stores those same rules. EX1003, ¶76. Alternatively and furthermore, a POSITA would also have found it obvious, based on the aforementioned teachings of Couillard in view of Freund, that one way to configure policies would be utilizing a server-based user interface such as that depicted by Freund, for a centrally located user interface to manage policies system-wide. EX1003, ¶76.

Thus, the Couillard-Freund combination teaches or at least renders obvious "providing a user interface, at a computing system remote from the end point, configured to allow configuration of a plurality of policies," as recited in 1[a]. EX1003, ¶77.

1[b]

The Couillard- Freund combination teaches 1[b] or at least renders 1[b] obvious. EX1003, ¶¶78-80. Couillard describes a "Block and Scan" method that "consists in 'Blocking' any workstation from entering the corporate network, that is blocking it before it obtains an IP address, and 'Scanning' it to make sure it is ***compliant with corporate policies (operating systems, hot fixes, security patches, antivirus software, etc.)***." EX1004, [0014]. As described with respect to 1[a], *supra*, Couillard teaches that the actions of the system "are performed based on the compliancy scanning results and depend on the ***security policies programmed in the CAS*** by the corporate network administrators and security analysts." EX1004, [0045]. Thus, these policies define "what is allowed, what is tolerated and what is blocked, in terms of antivirus software, operating systems, and associated security patches and signature files," etc. EX1004, [0014], [0048].

Couillard describes that these security policies can comprise Corporate Compliancy Rules (CCRs). EX1004, [0064]; EX1003, ¶79. For example, Couillard describes that the CCRs are each "a compliancy process through which is

checked a state of the device." EX1004, [0064]. Consistent with Couillard's description of the security policies, Couillard describes that the CCRs may, for example, "include[] information concerning all the OS patches, the Antivirus, the spyware, the versions of any piece of software, etc." EX1004, [0064]. "The state can be the presence or absence of any information on the device." EX1004, [0064]. The CCRs may include both detection rules (a "rule which is able to identify different characteristics of the device") and compliancy rules (a rule that "can be the presence or the absence or the status of" various conditions of the device). *See* EX1004, [0129]-[0156]. "For example, in the case a Norton Antivirus software was detected in the detection rule, a version and signature file may be checked in the compliance rule to ensure that the proper virus definitions are used by the device." EX1004, [0156]. Thus, a "plurality of policies," as recited in 1[b], is shown by at least any of the following: (1) detection rules, (2) compliancy rules, or (3) sets of rules applicable to different communities. EX1004, [0099], [0110]-[0111], [0127-128], [0142]-[0143], [0198] (discussing sets of rules). EX1003, ¶79.

The plurality of policies are maintained in a data store on the computing system. EX1003, ¶80. Couillard teaches that the Compliancy Appliance Server (CAS) side 76 is preferably designed as a "UNIX-O/S based appliance (OpenBSD ver, 3.5) for the Network Kernel built on carrier-grade Intel servers with redundant

components (power Supplies, fans, ***hardware-based RAID storage***, network interface cards)." EX1004, [0055]-[0056]. As shown in FIG. 3, Couillard teaches that the CAS includes compliance rules 79 (i.e., CCRs), and later describes that, once the CCRs have been defined by the administrator, they "***are stored in the Compliancy Appliance Server (CAS)***." EX1004, [0065]-[0066]; *see also* [0130], [0142] (CAS sends detection and compliancy rules to CSA). The CCRs "can be any electronic format of data sitting on a Computer hard disk device or in a memory of a Computer device." EX1004, [0064].

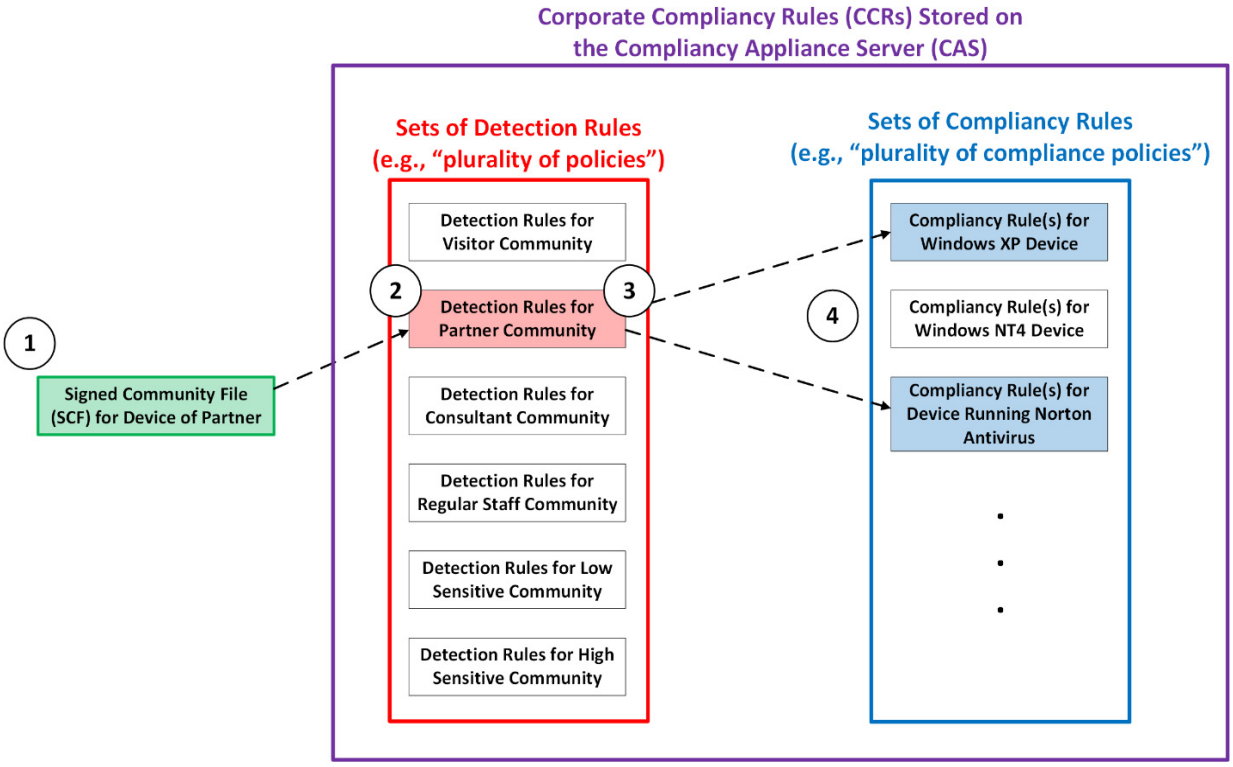
1[c]

The Couillard- Freund combination teaches 1[c] or at least renders 1[c] obvious. EX1003, ¶¶81-86. For example, Couillard describes that every time a device attempts to sign into the corporate network via the CAS, the CAS asks the CSA on the device to submit a Signed Community File (SCF). EX1004, [0098]; EX1003, ¶81. "The SCF is a signed file allowing the CAS to determine which community the device is identified to and therefore which set of compliancy rules [i.e., CCRs] applies." EX1004, [0099]. An administrator can "define as many communities as the corporation needs." EX1004, [0100]. For example, for the "Partner" community, "the devices are allowed to enter on the corporate network frequently but are not allowed to access sensitive resources," so a "single <<presence of>> Antivirus software [rule] may be sufficient." EX1004, [0108]. On the other hand, for the

regular staff community, "the set of compliancy rules for this community will be much more thorough than that of visitors, consultants or partners because the staff will have access to most of the corporate network resources and confidential corporate information like client files." EX1004, [0110].

Couillard describes that the first set of rules applicable for the submitted SCF that are sent to the CSA of the device requesting access to the corporate network are "detection rules." *See* EX1004, [0129]-[0130]; EX1003, ¶82. As described above, the "detection rule is a rule which is able to identify different characteristics of the device such as" the presence or the absence of "[a]ny Operating System (O/S) type and version," "[a]ny Antivirus Software installed," or "[a]ny running process on the device." EX1004, [0130]-[0132]. "The detection rules are used to tell the CAS on what type of device the compliance verification will be performed." EX1004, [0142]. "CSA sends the results of detection rules and CAS analyses the detection rule results, and determine[s] and sends to the CSA the proper set of <<compliancy>> rules to check on the device." EX1004, [0142]. Couillard identifies various operating conditions that can be monitored with compliancy rules, with results sent from the CSA to CAS for analysis. EX1004, [0143]-[0158].

The following diagram illustrates the sets of policies stored in the CAS and how each is selected for a given device requesting access to the corporate network:



EX1003, ¶83. Thus, (1) the CSA of a device requesting access sends its Signed Community File (SCF) to the CAS (*see* EX1004, [0098]-[0112], [0197]); (2) the CAS selects a set of detection rules applicable for the submitted SCF to the CSA of the requesting device (*see* EX1004, [0129]-[0141], [0197]); (3) CSA sends the results of detection rules and CAS analyses the detection rule results (*see* EX1004, [0142], [0197]); (4) the CAS determines and sends to the CSA the proper set of compliancy rules to check on the requesting device (*see* EX1004, [0142]-[0156], [0198]); and (5) the CSA checks the compliancy rules and sends results to the CAS for determination of compliance (EX1004, [0157]-[0158]). EX1003, ¶83.

A POSITA would have understood or at least found it obvious that the detection rules and/or compliancy rules include a plurality of operating conditions on

the endpoint (e.g., installed antivirus software, running processes, registry key data and state, firewall activation, signature files, etc.) to monitor on the device. *See* EX1004, [0130]-[0146]; EX1003, ¶84; *see also* EX1004, [0051] ("the CAS also provides corporate IT personnel the ability to ***monitor*** and control the entire corporate fleet of devices…."). Couillard further discloses that "as soon as a required rule is not complied with by a device, the device is deemed non-compliant," with an option to notify end-users "when their workstations are 'no longer' compliant," and that the "process is repeated until the device is deemed compliant," such as through correcting the non-compliant state (e.g., missing running process or antivirus software). EX1004, [0050]-[0051], [0061], EX1003, ¶84.

Moreover, it would have been alternatively obvious to a POSITA to configure the CSA to continuously monitor operating conditions specified in the detection rules and associated compliancy rules, after an initial verification, because a POSITA would have known that the state of a device is often continuously changing during its operation and that such changes may render the device non-compliant or alter the relevant compliancy rules. *See, e.g.*, EX1004, [0050] (describing the ability of the CAS to notify end-users when their workstations are no longer compliant); EX1005, 4:5-28 (describing ongoing rules that need to be continuously monitored, such as the "total time a user can be connected," and that some rules may be enforced at certain times of day); EX1003, ¶85. Moreover, as described in

greater detail below with respect to 1[g], Couillard describes that non-compliant devices are given an opportunity to remediate issues and recheck their verification state, which would lead to multiple, successive checks of the operating conditions identified in the detection rules and associated compliancy rules. *See* EX1004, [0061], [01609]-[0163], [0190]-[0195]; EX1003, ¶85. Thus, a POSITA would have been motivated to implement Couillard's CAS and CSA to continuously monitor the operating conditions of the detection rules and associated compliancy rules, because it would have ensured ongoing security of the corporate network. EX1003, ¶85.

Thus, when the CAS identifies the set of detection rules applicable for the SCF submitted by the CSA of a device requesting access, and/or the applicable compliancy rules, a POSITA would have understood or at least found it obvious that the CAS is "identifying, from the plurality of policies [i.e., all detection rules and/or compliancy rules for all communities], a plurality of operating conditions on the endpoint to monitor [i.e., the operating conditions specified in the detection rules and/or compliancy rules applicable for the community to which the SCF of the requesting device is associated]," as recited in 1[c]. *See* EX1004, [0142]-[0156]; EX1003, ¶86.

1[d]

The Couillard-Freund combination teaches 1[d] or at least renders 1[d] obvious. EX1003, ¶¶87-92.

Couillard generally teaches that the "CSA verifies the compliance of each rule in the set of rules transmitted by the CAS." EX1004, [0143]. FIG. 3 illustrates the CSA as including various components, such as a compliance verifier 72 that "obtain[s] the compliance verification results." EX1004, [0043]. However, as described in Sections IV.A.1 and 3, *supra*, Couillard does not dictate or otherwise limit the form that the CSA takes, such as the implementation details of the compliance verifier 72 or how it "obtain[s] the compliance verification results." *See id.*; EX1003, ¶87.

Thus, for at least the reasons described in Section IV.A.3, *supra*, a POSITA would have found it obvious to look to Freund (e.g., the implementation of Freund's monitor and data acquisition module 440 and associated hooks) to provide at least one obvious implementation of an element of the CSA for collecting data about the operating conditions specified in the CCRs (and/or compliancy rules and/or detection rules). EX1003, ¶88. Like Couillard, Freund's system includes two main components: "a client-based filter application (installed at each client), and a central supervisor application that maintains the access rules for the client based filter and verifies the existence and proper operation of the client-based filter

application." EX1005, FIG. 3A, 12:45-65, 14:52-15:11; EX1004, FIG. 3, [0040]; EX1003, ¶88. "The client-based filter application, which in a preferred embodiment performs all of the monitoring, logging, and filtering work, is responsible for intercepting process loading and unloading," as well as "keeping a list of currently active processes; . . . [and] intercepting and interpreting all TCP/IP communication and build[ing] a comprehensive representation of these TCP/IP activities." EX1005, 13:23-33.

To perform the "monitoring, logging, and filtering work," Freund's client-based filter application includes a data acquisition module 440, which is illustrated and described with respect to FIGS. 4 and 5. *See* EX1005, 15:12-16:29, 20:50-21:46; EX1003, ¶89. The data acquisition module 440, which is preferably implemented as a Windows VxD driver, includes several "hooks" that allow the data acquisition module 440 to hook into various operating system components. EX1005, 20:50-63. For example, data acquisition module 440 includes a "File Hook 503" that "includes functionality allowing the driver 440 to ***hook into the file subsystem provided by the underlying operating system***." EX1005, 20:54-57. Similarly, "Process Hook 505" is a subcomponent that "***hooks into the underlying operating system***, [and] tracks all currently-executing applications or processes." EX1005, 20:57-60. Each of these hooks "are capable of executing at ring 0--that is, execution at the highest privileged level of the operating system." EX1005, 20:60-63.

A POSITA would have known that:

> In the Microsoft Windows operating system, a hook is a mechanism by which a function can intercept events (messages, mouse actions, keystrokes) before they reach an application. The function can act on events and can, in some cases, modify or discard these events. Functions that receive events are called filter functions and are classified according to the type of event they intercept. . . . ***For Windows, the filter function must be installed—that is, attached—to a Windows hook (for example, to a keyboard hook) to be called. Attaching one or more filter functions to a hook is known as setting a hook***. . . . The Win32® (a trademark of Microsoft Corporation) Application Programming Interface (API) ***provides a set of functions to access and modify***: the z-order list; the windows position and styles; and the hook operating system mechanism. . . . In the Microsoft Windows Operating System environment, a Hook Filter is a dynamic library registered at the system level. To set such filter, it is necessary to initialise and ***configure the Hook mechanism using the SetWindowsHook Win32® API*** (Application Programming Interface).

EX1008, 4:52-4:5, 6:5-12.

Based on these teachings and for the reasons outlined in Section IV.A.3, *supra*, a POSITA would have found it obvious to implement at least one element of Couillard's CSA (e.g., the compliance verifier 72 or a portion thereof) to collect at least a portion of the data about the operating conditions specified in the CCRs (and/or detection rules and/or compliancy rules) in association with step 126 and/or

127 of Couillard's FIG. 6 by setting one or more hooks into the operating system of the device on which the CSA is installed. EX1003, ¶91. Having set these hooks, the CSA would have been able to "intercept[] process loading and unloading and keep[] a list of currently active processes," which would have allowed the CSA to "check[] for various characteristics, including checking ***executable names, version numbers***, executable file checksums, version header details, ***configuration settings***, and the like," as taught by Freund. EX1005, 13:34-39. In this manner, having received the appropriate CCRs (and/or detection rules and/or compliancy rules) from the CSA, Couillard's CSA would thus have been configured via the CCRs (and/or detection rules and/or compliancy rules) to monitor various characteristics with respect to the CCRs (and/or detection rules and/or compliancy rules) being evaluated by the CSA and CAS for compliancy, and for the operating conditions specified in Couillard. *See* EX1004, [0129]-[0156] (describing step 126 of verifying compliance of a device); EX1003, ¶91.

Under this obvious implementation of the combined teachings of Couillard and Freund, Couillard's CSA itself would be "one or more software agents on the endpoint" that is configured "to monitor the plurality of operating conditions," as recited in 1[d]. EX1003, ¶92. Furthermore, Couillard's teachings alone regarding configuring the CSA to monitor the aforementioned operating conditions specified

in any of the CCRs, detection rules, and/or compliancy rules would satisfy 1[d], without the teachings of Freund. EX1003, ¶92.

1[e]

The Couillard-Freund combination teaches 1[e] or at least renders 1[e] obvious. EX1003, ¶¶93-95. For instance, Couillard teaches that, after the CSA verifies compliance for the device for each rule applicable for the submitted SCF in step 126 of FIG. 6, the "CSA transmits a message to CAS containing the result of compliance verification for each rule." EX1004, FIG. 6, [0157]-[0158]. The "CSA, after checking all the compliancy rules status, transmits to CAS the results of each rule." EX1004, [0158]. The results sent to the CAS show the claimed status information about the plurality of operating conditions. EX1003, ¶93.

Couillard teaches that the CAS receives status information about operating conditions specified in each of the detection and compliancy rules. EX1003, ¶94. As described with respect to 1[b], the CCRs include both the detection rules (a "rule which is able to identify different characteristics of the device") and the compliancy rules (a rule that "can be the presence or the absence or the status of" various conditions of the device). *See* EX1004, [0129]-[0156]. As shown in FIG. 6 and explained with respect to steps 125 and 126, Couillard teaches that the proper set of compliancy rules to evaluate on the device is determined from the detection rules. *See* EX1004, [0142]. Thus, as described with respect to 1[c], the CSA first

sends status information associated with the detection rules to the CAS to get the proper set of compliancy rules. *See* EX1004, [0142]. Thereafter, the "CSA verifies the compliance of each rule in the set of rules transmitted by the CAS," and "transmits a message to CAS containing the result of compliance verification for each rule [i.e., status information about the operating conditions specified in the compliancy rules]." *See* EX1004, [0143]-[0158]; EX1003, ¶94.

Here, the "computing system" recited in 1[e] includes at least the Compliancy Appliance Server (CAS) side 76, the "endpoint" recited in 1[e] is the device requesting access to the corporate network, and the "one or more software agents" that gather the "status information about the plurality of operating conditions" recited in 1[e] are the Compliancy Security Agent (CSA) side 70 in conjunction with the hooks it sets in view of Freund (or alternatively without the hooks based on Couillard alone), as described with respect to 1[d]. EX1003, ¶95. The communications between the CAS and the CSA happen over a Secure Sockets Layer (SSL) connection via the CSA's network (e.g., TCP/IP connection 53), and therefore happen "across a network," as recited in 1[e]. *See* EX1004, FIG. 2, [0041], [0071]-[0072], [0096]-[0097]; EX1003, ¶95.

1[f]

The Couillard-Freund combination teaches 1[f] or at least renders 1[f] obvious. EX1003, ¶¶96-100. For example, Couillard describes that the "CSA, after

checking all the compliancy rules status, transmits to CAS the results of each rule." EX1004, [0157]-[0158]. Then, Couillard describes that, in step 128, the "CAS analyses [the results from the CSA] and decides if the device is compliant or not with the rules." EX1004, [0159]-[0164]. "The CAS decision about the compliancy is to check if all required rules are respected." EX1004, [0163]. "A required rule is a rule where a non compliancy will block the device from logging onto the network." EX1004, [0162].

Couillard provides an example:

> [A] compliant device could be defined by a network administrator as a device having its O/S up to date with the latest Security OS patches from the manufacturer plus an Antivirus Software version up to date and up and running with the last signature file from the Antivirus manufacturer. In this example, the CAS would have four required rules. One rule for the O/S patches, one rule for the Antivirus Software version, one rule to confirm if the Antivirus is running of the device and the last one to check if the Antivirus has the latest virus signature file from the Antivirus manufacturer. A compliant device will have a successful compliancy verification if all four compliancy rules are respected. The CAS analyses all the rules and make the compliancy decision.

EX1004, [0163]-[0164].

In this example, the CAS "determin[es] . . . a compliance state of the endpoint based on the status information and a plurality of compliance policies [e.g.,

the four required rules] in the data store," as recited in 1[f]. EX1003, ¶98. The "compliance state of the endpoint" would be the determination by the CAS of whether "the device is compliant or not with the compliancy rules" (e.g., "O/S up to date with the latest Security OS patches from the manufacturer") and whether each rule is an "informative," "advisable," or "mandatory" rule. *See* EX1004, [0159]-[0163]; EX1003, ¶98. The "status information" is the message transmitted from the CSA to the CAS containing the results of the compliance verification for each rule. *See* EX1004, [0157]-[0158]. And the "plurality of compliance policies in the data store" are the proper set of compliancy rules checked by the CSA, which as noted in 1[b] are stored in the data store. *See* EX1004, [0142]-[0158]; EX1003, ¶98.

The compliance state of the endpoint is "based on" the status information received with respect to each of the detection and compliancy rules. EX1003, ¶99. As described with respect to 1[b], the CCRs include both the detection rules (a "rule which is able to identify different characteristics of the device") and the compliancy rules (a rule that "can be the presence or the absence or the status of" various conditions of the device). *See* EX1004, [0129]-[0156]. As shown in FIG. 6 and explained with respect to steps 125 and 126, Couillard teaches that the proper set of compliancy rules to evaluate on the device is determined from the detection rules. *See* EX1004, [0142]. Thus, as described with respect to 1[c], the CSA first

sends status information associated with the detection rules to the CAS to get the proper set of compliancy rules. *See* EX1004, [0142]. Thereafter, the "CSA verifies the compliance of each rule in the set of rules transmitted by the CAS," and "transmits a message to CAS containing the result of compliance verification for each rule [i.e., the compliancy rules associated with the detection rules]," which the CAS "analyses and decides if the device is compliant or not with the rules." *See* EX1004, [0143]-[0159], [0163]-[0164]. Because the status information associated with the compliancy rules is sent by the CSA after and as a result of the initial status information associated with the detection rules, the compliance state of the endpoint is "based on" the status information received by the CAS from the CSA with respect to each of the detection and compliancy rules. *See generally* EX1004, [0127]-[0159], [0163]-[0164]; EX1003, ¶99.

Couillard describes that "[c]ompliancy rules can be the presence or the absence or the status of," for example, "[a]ny Operating System (O/S) type and version," configuration data, antivirus version, and/or "[a]ny software status (i.e. Antivirus is up and running, personal firewall is activated, etc.)." *See* EX1004, [0144]-[0155]. Accordingly, these compliancy rules include the items on an endpoint to monitor, the analysis methods to use, and the permitted thresholds for the monitored items. *See* EX1004, [0144]-[0155]; EX1003, ¶100.

1[g]

The Couillard-Freund combination teaches 1[g] or at least renders 1[g] obvious. EX1003, ¶¶101-107. As described with respect to 1[f], *supra*, Couillard's "CAS analyses and decides if the device is compliant or not with the rules." EX1004, [0159]-[0164]. Couillard describes that the "CAS can manage many different types of rules." EX1004, [0161]. One type of rule is a "required rule," which "is a rule where a non compliancy will block the device from logging onto the network." EX1004, [0162]. If the CAS determines that a device is not in compliance with a "required rule," the "device is then put in quarantine until the time a remediation is applied." EX1004, [0162]. On the other hand, if the CAS determines that a device is compliant with all of the applicable rules, the CAS assigns the device to the "production VLAN," where it gains access to the corporate network and associated resources. *See* EX1004, [0044]-[0045], [0165]-[0167]; EX1003, ¶101.

To put a device into any of the production, quarantine, or restricted VLANs, the CAS "sends a <<change VLAN>> request to CAS SNMP server with the device MAC address and device production VLAN assignment." EX1004, [0166], [0192]. As part of the process of sending the device to a different VLAN, the "CAS instructs CSA to close the SSL connection and to make an IP address release and wait a number of second[s] then start an IP address renew." *See* EX1004,

[0175]; EX1003, ¶102. Thus, a first action that the CAS remotely initiates based on the compliance state is to cause a processor of the device (endpoint) to assist in moving the device to the appropriate separate VLAN. EX1003, ¶102.

A POSITA would have understood or at least found it obvious that this action (i.e., the instruction to "close the SSL connection and to make an IP address release and wait a number of second then start an IP address renew") would have been "identified in at least one rule in the data store," as recited in 1[g], such as the exemplary RAID storage on the CAS. EX1004, [0053], [0065]-[0066], EX1003, ¶103. For example, policies and compliance policies are already stored on the CAS, and compliance is determined by the CAS. *See* EX1004, [0065]-[0066], [0157]-[0164]; EX1003, ¶103. The instruction from the CAS to the endpoint is a rule (or part of a rule) based on the compliance determination. *See* EX1004, [0160]-[0162], [0165]-[0167], [0190]-[0193]; EX1003, ¶103. All of this amounts to instructions that govern the CAS's operation. Thus, the rule implemented by the CAS would be stored on the CAS data store, just like the compliancy rules, as described with respect to 1[b] and 1[f]. EX1003, ¶103.

Furthermore, Couillard teaches that each of the Corporate Compliancy Rules (CCRs) is "a compliancy ***process*** through which is checked a state of the device." EX1004, [0064]. A POSITA would have understood or at least found it obvious

that one step in this stored "process" would have been the resulting action (e.g., remediation instructions, VLAN directions, notifications) from compliance/non-compliance with the policy, and thus the action is within the compliance rule (or at least a rule) in the data store. EX1003, ¶104**.** Moreover, Couillard teaches that the "CAS can manage many different types of rules," and describes that different rules can be associated with different actions/outcomes. *See* EX1004, [0160]-[0162]; EX1003, ¶104. Thus, a POSITA would have at least found it obvious that one straightforward way to associate each rule or rule type with the appropriate action/outcome would be for the action to be "identified in at least one rule in the data store," as recited in 1[g], because this approach would avoid the need to maintain and access more than one source of data and avoid the need provide logical links between those data stores. EX1003, ¶104. A POSITA also would have been motivated with a reasonable expectation of success because it is logical for the CAS, which already makes the compliance determinations and implements rules based on it, to store the rules in the same storage as the compliance policies. EX1003, ¶104.

Beyond moving the device to a particular VLAN, another action that the CAS remotely initiates based on the compliance state of the device is to initiate remediation. *See* EX1004, [0061], [0161]-[0162]. Specifically, Couillard teaches

that "[t]he only way to make [a non-compliant] device compliant again is by having the device go through the same compliancy verification process" after "[c]orrections are made to the device." *See* EX1004, [0061]; EX1003, ¶105. "***The corrections (remediation) can be made*** manually or ***automatically*** depending on the network settings." EX1004, [0061]. The CAS can also provide a notification of non-compliance. EX1004, [0050].

In one example, Couillard describes that the "device can also be fixed with a CAS automated integrated patch management tool." EX1004, [0162]. In other words, the CAS automatically fixes the non-compliant device via the integrated patch management tool. EX1003, ¶106. A POSITA would have understood or at least found it obvious that the automatic remediation provided by Couillard's CAS includes "initiating, by the computing system [i.e., at least Couillard's CAS], based on the compliance state, an action [i.e., automatic remediation and/or user notification]. . . , wherein the action is carried out by a processor on the endpoint [i.e., the processor of the non-compliant device installing the patch or other remediation, or displaying the notification, received from the CAS]," as recited in 1[g]. EX1003, ¶106.

Furthermore, a POSITA would have understood or at least found it obvious that the action would have been "identified in at least one rule in the data store" for the reasons described with respect to the VLAN action above. EX1003, ¶107.

Furthermore, because remediation for any given rule is often associated with that rule (*see, e.g.*, EX1004, [0160]-[0162]), a POSITA would have understood or at least found it obvious that a remediation action would also have been "identified in at least one rule in the data store," as recited in 1[g]. EX1003, ¶107. For example, Couillard describes that one required rule could be "to check if the Antivirus has the latest virus signature file from the Antivirus manufacturer." EX1004, [0163]. The remediation for this rule would be to download and install the latest virus signature file, which is an action directly tied to this particular rule. *See* EX1004, [0162]-[0163]; EX1003, ¶107. In at least this example from Couillard, a POSITA would have understood or at least found it obvious that the action (i.e., automatically downloading and installing the latest virus signature file) would have been "identified in at least one rule in the data store" (i.e., the required rule that "the Antivirus has the latest virus signature file from the Antivirus manufacturer" or at least a rule based on the outcome of that determination), as recited in 1[g]. EX1003, ¶107.

(ii) Claim 23

23[pre]

Limitation 23[pre] is substantively similar to limitation 1[pre] and is therefore taught by or at least rendered obvious by the combination of Couillard and Freund for at least the same reasons described above with respect to 1[pre].

EX1003, ¶110. Furthermore, Couillard teaches that its invention provides "a ***system*** for verifying compliance of a device wanting to access a corporate network and OSI layer 2 connecting of the device using the compliance verification." EX1004, [0017]. The system taught by Couillard that provides the functionality described with respect to claim 1 is illustrated in at least FIGS. 2 and 3. EX1004, [0021]-[0022], [0040]-[0044]; EX1003, ¶110.

23[a]

Limitation 23[a] is substantively similar to limitation 1[a] and is therefore taught by or at least render obvious by the combination of Couillard and Freund for at least the same reasons described above with respect to 1[a]. EX1003, ¶111.

23[b]

Limitation 23[b] is substantively similar to limitation 1[b] and is therefore taught by or at least render obvious by the combination of Couillard and Freund for at least the same reasons described above with respect to 1[b]. EX1003, ¶112.

23[c]

Limitation 23[c] is substantively similar to limitation 1[d] and is therefore taught by or at least rendered obvious by the combination of Couillard and Freund for at least the same reasons described above with respect to 1[d]. EX1003, ¶113.

23[d]

The Couillard-Freund combination teaches 23[d] or at least renders 23[d] obvious. EX1003, ¶114. For example, Couillard teaches that the Compliancy Appliance Server (CAS) side 76 is preferably designed as a "UNIX-O/S based appliance (OpenBSD ver, 3.5) for the Network Kernel built on carrier-grade ***Intel servers*** with redundant components (power Supplies, fans, hardware-based RAID storage, network interface cards)." EX1004, [0055]-[0056]. As described with respect to 11[pre], Intel servers running UNIX-O/S were known to employ Intel processors executing computer instructions stored on a computer readable medium (e.g., in the RAID storage). EX1003, ¶114. Thus, a POSITA would have known or at least found it obvious that Couillard's CAS included "one or more hardware processors at the computing system configured to" perform the various functions described with respect to the CAS and elements 23[d.i]-[d.iii], and indeed a PHOSITA would have known that such computer functions were ordinarily carried out by hardware processor configured to implement them. EX1003, ¶114.

23[d.i]

Limitation 23[d.i] is substantively similar to limitation 1[e] and is therefore taught by or at least rendered obvious by the combination of Couillard and Freund for at least the same reasons described above with respect to 1[e]. EX1003, ¶115.

23[d.ii]

Limitation 23[d.ii] is substantively similar to limitation 1[f] and is therefore taught by or at least rendered obvious by the combination of Couillard and Freund for at least the same reasons described above with respect to 1[f]. EX1003, ¶116.

23[d.iii]

Limitation 23[d.iii] is substantively similar to limitation 1[g] and is therefore taught by or at least rendered obvious by the combination of Couillard and Freund for at least the same reasons described above with respect to 1[g]. EX1003, ¶117.

(iii) Claim 25

The Couillard-Freund combination teaches [25] or at least renders [25] obvious. EX1003, ¶¶119-120. As described with respect to 1[a], *supra*, in order to program the security policies into the CAS, Couillard teaches that the "system is preferably accessible within an ***administrator management interface***, such as the Microsoft-based Management Console (MMC), which network and system administrators are already familiar with and use on a daily basis to monitor, manage and query desktops, laptops, servers, networks and other LAN resources." EX1004, [0053]. As further described with respect to 1[a], it would have been obvious that at least one logical component of Couillard's system to host/execute the administrator management interface would be the CAS (or at least a component of the

computing system that includes the CAS), and that Freund provides exemplary descriptions of user interfaces for configuring policies. *See* EX1004, [0045], [0053]; EX1005, 12:45-14:12, 14:52-15:11; EX1003, ¶119.

Further, it would have been obvious as of the Critical Date that administrator management interfaces could be implemented as a web interface to permit remote access through a web page (as an alternative to or in conjunction with the Microsoft-based Management Console (MMC)). *See, e.g.*, EX1006, [0101]-[0106]; EX1007, 9:14-26; *see also* EX1004, [0161] (describing the provision of compliancy information via a webpage, suggesting access to the compliancy system via web page); EX1003, ¶120. Web page-based interfaces were very well known by the 2005 Critical Date. EX1003, ¶120. A POSITA would have been motivated to implement the administrator management interface to comprise a webpage, because it would have permitted remote access to the administrator management interface, not required the administrator to be physically present at the CAS that hosts/executes the administrator management interface, provides ability to readily update the interface through known web-based languages, could provide an interface accessible without installing additional software on a computer accessing the interface, and could provide an interface compatible with different types of hardware and software configurations without needing to program the interface specifically for each (e.g., a web-based interface may run on various operating systems

and hardware without modifying interface code). EX1004, [0009] (describing that wireless access to the corporate network and its associated resources—*e.g.*, the administrator management interface –enhances productivity); EX1003, ¶120. A POSITA would have had a reasonable expectation of success implementing this predictable interface. *See, e.g.*, EX1006, [0101]-[0106]; EX1007, 9:14-26; *see also* EX1004, [0161] (describing the provision of compliancy information via a webpage, suggesting access to the compliancy system via web page); EX1003, ¶120. Thus, a POSITA would have understood or at least found it obvious based on the teachings of Couillard and their own knowledge that Couillard's administrator management interface would have included a web page for configuring policies. EX1003, ¶120.

(iv) Claim 31

The Couillard-Freund combination teaches [31] or at least renders [31] obvious. EX1003, ¶¶122-123. As described with respect to 1[f], Couillard describes that, in step 128, the "CAS analyses and decides if the device is compliant or not with the rules." EX1004, [0159]-[0164]. "The CAS decision about the compliancy is to check if all required rules are respected." EX1004, [0163]. "A required rule is a rule where a non compliancy will block the device from logging onto the network." EX1004, [0162].

Couillard provides an example:

> [A] compliant device could be defined by a network administrator as a device having its O/S up to date with the latest Security OS patches from the manufacturer plus an Antivirus Software version up to date and up and running with the last signature file from the Antivirus manufacturer. In this example, the CAS would have four required rules. One rule for the O/S patches, one rule for the Antivirus Software version, one rule to confirm if the Antivirus is running of the device and the last one to check if the Antivirus has the latest virus signature file from the Antivirus manufacturer. A compliant device will have a successful compliancy verification if all four compliancy rules are respected. The CAS analyses all the rules and make the compliancy decision.

EX1004, [0163]-[0164]. In this example, a POSITA would have understood or at least found it obvious that at least the rules for "confirm[ing] if the Antivirus is running of the device," OS and antivirus version, and "check[ing] if the Antivirus has the latest virus signature file from the Antivirus manufacturer" are "software conditions," as recited in [8], because they are conditions of software. EX1003, ¶123. Furthermore, software conditions for detection rules and/or compliancy rules include at least presence, absence, or status of: antivirus software installed, registry key data and state, spyware, file format or program size/date stamp/folder location, running processes, set up and configuration data, and software status (e.g., is antivirus or firewall running). EX1004, [0130]-[0156].

(v) Claim 33

The Couillard-Freund combination teaches [33] or at least renders [33] obvious. EX1003, ¶¶125-128. Couillard teaches that the actions of the system "are performed based on the com-pliancy scanning results and depend on the ***security policies programmed in the CAS*** by the corporate network administrators and security analysts." EX1004, [0045]. As described with respect to 1[b], *supra*, Couillard describes that these security policies can comprise Corporate Compliancy Rules (CCRs). EX1004, [0064]. For example, Couillard describes that the CCRs are each "a compliancy process through which is checked a state of the device." EX1004, [0064]. Consistent with Couillard's description of the security policies, Couillard describes that the CCRs may, for example, "include[] information concerning all the OS patches, the Antivirus, the spyware, the versions of any piece of software, etc." EX1004, [0064]. "The state can be the presence or absence of any information on the device." EX1004, [0064]. The CCRs may include both detection rules (a "rule which is able to identify different characteristics of the device") and compliancy rules (a rule that "can be the presence or the absence or the status of" various conditions of the device). *See* EX1004, [0129]-[0156]. "For example, in the case a Norton Antivirus software was detected in the detection rule, a version and signature file may be checked in the compliance rule to ensure that the

proper virus definitions are used by the device." EX1004, [0156]. Thus, a "plurality of policies," as recited in 1[b], is shown by at least any of the following: (1) detection rules, (2) compliancy rules, or (3) sets of rules applicable to different communities. EX1004, [0099], [0110]-[0111], [0127-128], [0142]-[0143], [0198] (discussing sets of rules). EX1003, ¶125.

Furthermore, as described with respect to 1[g], Couillard teaches that each of the Corporate Compliancy Rules (CCRs) is "a compliancy ***process*** through which is checked a state of the device." EX1004, [0064]. A POSITA would have understood or at least found it obvious that one step in this stored "process" would have been the resulting action (e.g., remediation instructions, VLAN directions, notifications) from compliance/ non-compliance with the policy, and thus the action is within compliance rule (or at least a rule) in the data store. EX1003, ¶126. Moreover, Couillard teaches that the "CAS can manage many different types of rules," and describes that different rules can be associated with different actions/outcomes. *See* EX1004, [0160]-[0162]; EX1003, ¶126. Thus, a POSITA would have at least found it obvious that one straightforward way to associate each rule or rule type with the appropriate action/outcome would be for policies (detection rules, compliancy rules, CCRs) to "include the at least one rule that identifies the action," because this is a logical organization of the data and avoid the need to maintain and

access more than one source of data and avoid the need provide logical links between those data stores. EX1003, ¶126.

Furthermore, as described for 1[g], Couillard describes multiple possible actions to take in response to a compliance determination (e.g., directing the endpoint to a particular VLAN, automatic remediation, notifications). *See* EX1004, [0160]-[0162], [0165]-[0179]; EX1003, ¶127. Couillard explains that "the CAS allows organizations to easily and rapidly define their workstation compliancy policies," and "once defined, the CAS provides corporate network administrators and security analysts the ability to publish and ***enforce*** predefined workstation compliancy policies." EX1004, [0048]-[0049]. A POSITA would have understood from this language that the enforcement rules that identify actions for remediation, notification, and/or VLAN direction are themselves part of the policies, or at least would have found the language and common sense to suggest that obvious solution so that the consequences of compliance/non-compliance were logically organized and associated with the rules that are used to define compliance. EX1003, ¶127. A POSITA also would have been motivated because it is common sense to allow administrators freedom to specify actions specific to particular policies (e.g., that violating a policy with an outdated software version should result in patching it to a specified version, that a particular policy violation should result in an endpoint being di-

rected to a quarantined VLAN instead of a restricted VLAN, etc.), with a reasonable expectation of success as this involves only predictable use of well-known programming techniques. *See* EX1004, [0045] (noting non-compliant endpoints may be directed to restricted VLANs or quarantine VLANs); EX1003, ¶127.

From at least these teachings, a POSITA would have understood or at least found it obvious that "the plurality of policies includes at least one policy that includes the at least one rule that identifies the action," as recited in [10]. EX1003, ¶128.

V. PTAB DISCRETION SHOULD NOT PRECLUDE INSTITUTION

A. The *Fintiv* Factors Favor Institution—§314(a)

Institution is consistent with the Director's recent guidance on applying the *Fintiv* Factors. *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020) (precedential) ("*Fintiv I*"); EX1101 ("*Director's Memo*").

Beginning on August 3, 2022, pursuant to 28 U.S.C. §1407(a), the United States Judicial Panel on Multidistrict Litigation ("MDL Panel") centralized several litigations from various districts involving Patent Owner Taasera in the Eastern District of Texas ("EDTX"), including the litigation involving the parties to this proceeding. EX1100. The centralized proceedings were assigned to Judge Gilstrap for pretrial management only and must be statutorily remanded to the originating court before trial. 28 U.S.C. §1407(a) ("Each action so transferred shall be remanded by

the panel at or before the conclusion of such pretrial proceedings to the district from which it was transferred unless it shall have been previously terminated"). While Judge Gilstrap has set trial for EDTX cases on April 15, 2024, no trial has been set in the originating district. EX1102, 1 (noting the "trial date applies only to cases originally filed in [EDTX]"). Therefore, trial must be set by the eventual trial court pending that court's trial calendar after transfer back. Furthermore, the schedule in EDTX may also be extended. Petitioner also intends to file a motion to transfer the case to California once the case is remanded to the originating court, followed by a motion to stay the case at the originating court pending transfer determination and pending IPR, leaving a trial date even more uncertain.

Further, Petitioner stipulates that if instituted, Petitioner will not seek resolution in the District Court of any ground of invalidity for the '038 Patent that utilizes the prior art references relied upon in the grounds of the instant petition. Petitioner's proposal is comprehensive and addresses the concern of narrowing the issues, as this stipulation ensures there is no overlap between the '038 Patent invalidity theories before the Board and at issue in the District Court. Petitioner's proposed stipulation is far more restrictive than a *Sand Revolution* stipulation, which excludes only the same grounds advanced in the IPR, allowing the Petitioner to rely on the same references in the two tribunals so long as the reliance is not identical.

Therefore, with an unknown trial date and any overlap mitigated by stipulation, denial under § 314(a) is not warranted.

Further, "where the PTAB determines that the information presented at the institution stage presents a compelling unpatentability challenge, that determination alone demonstrates that the PTAB should not discretionarily deny institution under *Fintiv*." *Hewlett Packard Enterprise Co., et al. v. Billjco LLC*, IPR2022-00420, Paper 17, at 6 (PTAB July 12, 2022). The strength of Petitioner's proposed grounds presented above weighs strongly in favor of institution. *Id.*

B. § 325(d) Favors Institution

Couillard was not considered or cited in the prosecution of the '038 Patent, and consequently, is being considered for the first time in this IPR proceeding. Thus, none of the Grounds involve the same or substantially the same prior art or arguments previously presented to the Office. 35 U.S.C. § 325(d).

C. *General Plastic* Factors Favor Institution—§314(a)

The '038 Patent is currently being challenged in instituted IPR2023-00573 filed by Palo Alto Networks, Inc. ("PAN"). The instant petition is entirely distinct—it is being filed by an entirely separate party sued eight months after PAN, and this petition uses completely different prior art than was used in PAN's earlier petition. For these reasons, the *General Plastic* factors favor institution. *General Plastic Industrial Co. v. Canon Kabushiki Kaisha*, IPR2016-01357, Paper 19 at 16 (PTAB

Sept. 6, 2017) (precedential as to section II.B.4.i).

1. Factors 1, 2, 4, and 5: CrowdStrike and PAN Are Entirely Separate Entities

CrowdStrike and PAN are separate companies sued eight months apart by Patent Owner. The CrowdStrike and PAN products Patent Owner accuses of infringing the '038 Patent are not related to one another. Moreover, CrowdStrike and PAN did not cooperate in any way in preparing either the previously filed IPR2023-00573 or this petition. These facts are nearly opposite facts to those present in the Board's precedential Valve decision. *See Valve Corp. v. Elec. Scripting Prods., Inc.*, IPR2019-00062, Paper 11 at 9-10 (PTAB Apr. 2, 2019) (precedential).

Because the evidence does not show a significant relationship between CrowdStrike and PAN, "*General Plastic* factors 1, 2, 4, and 5 weigh against discretionary denial." *Volkswagen Group of America, Inc. v. Neo Wireless LLC*, IPR2022-01537, Paper 8 at 11 (PTAB May 5, 2023). Where, as here, "there is no indication of a significant relationship under *Valve* and factor 1 between Petitioner and the" prior petitioner, "Petitioner did not file a second petition following-on to a first petition under factors 2, 4, and 5." *Id.* "In other words, this is not a case where we need to address concerns that Petitioner is 'strategically stag[ing] [its] prior art and arguments in multiple petitions' in order to refine its positions based on lessons learned from Petitioner's filing of an earlier petition." *Id.* (citing *General Plastic*, Paper 19 at 17; *Code200, UAB v. Bright Data, Ltd.*, IPR2022- 00861, Paper 18 at 5

(PTAB Aug. 23, 2022) (precedential)).

2. Factor 3: Patent Owner's Staggered Litigation Strategy Precipitated the Staggered Filing of the Petitions

Patent Owner sued PAN for infringement of the '038 Patent on February 25, 2022. Nearly eight months later, Patent Owner sued CrowdStrike for infringement of the '038 Patent on October 21, 2022. PAN filed its petition against the '038 Patent (IPR2023-00573) on February 10, 2023. And, nearly eight months later, CrowdStrike is filing this petition. Thus, while the POPR and Institution Decision have issued in IPR2023-00573, the impact of this fact is mitigated by Patent Owner's nearly identically staggered assertion strategy. *See Volkswagen Group*, Paper 8 at 11.

3. Factors 6 and 7: The Distinct Grounds and Lack of Significant Relationship Ensure the Board's Resources and Ability to Render a Decision Within the Statutory Timeframe Are Not Significantly Impacted

There are no common prior art references between this petition and IPR2023-00573. Moreover, because CrowdStrike and PAN share no significant relationship, the rights of CrowdStrike to pursue this petition will not in any way be impacted by the outcome of IPR2023-00573. Thus, any Final Written Decision in IPR2023-00573 is unlikely to have a significant impact on the merits or conduct of an instituted IPR from this petition. And while the Board will expend resources necessary to hear this second petition, the expenditure of those resources is justified by

CrowdStrike's independent and distinct basis under §314 to file an IPR petition and the fees that CrowdStrike is paying to have this petition heard on the merits.

Furthermore, it's entirely possible for Patent Owner to settle with PAN and seek termination of IPR2023-00573 at any time during its pendency, after CrowdStrike's statutory bar date. CrowdStrike's basis under §314 to have the Board consider the patentability of the '038 Patent should not be put in tension with and potentially curtailed by Patent Owner and PAN's distinct right to settle their dispute outside of CrowdStrike's control.

In fact, efficiency and the integrity of the patent system are well served by the institution of this petition. The claims of the '038 Patent are very similar to the claims of U.S. Patent No. 9,608,997 (the '997 Patent). In parallel with this petition, Petitioner is filing a petition against the '997 Patent (i.e., IPR2023-01463), which is the first IPR petition filed against the '997 Patent. The same prior art relied upon in this petition is also at issue in IPR2023-01463. Thus, to the extent that IPR2023-01463 is instituted (where the *General Plastic* factors do not apply), the Board will already be considering substantially the same prior art and arguments against substantially the same claims. Accordingly, it would be an efficient use of the Board's resources and in the interests of the integrity of the patent system to institute both IPR2023-01463 and this petition.

VI. FEES

CrowdStrike Inc. authorizes the Patent and Trademark Office to charge Deposit Account No. 06-1050 for the fee set in 37 C.F.R. § 42.15(a) and for any additional fees.

VII. CONCLUSION

Petitioner requests cancellation of all Challenged Claims.

VIII. MANDATORY NOTICES UNDER 37 C.F.R § 42.8(a)(1)

A. Real Party-In-Interest Under 37 C.F.R. § 42.8(b)(1)

CrowdStrike Inc. and CrowdStrike Holdings, Inc. are the real parties-in-interest.

B. Related Matters Under 37 C.F.R. § 42.8(b)(2)

Petitioner is not aware of any terminal disclaimers or reexamination certificates for the '038 Patent. The '038 Patent is the subject of the following civil actions:

- *Taasera Licensing LLC v. Trend Micro Incorporated*, Case No. 2:21-cv00441 (EDTX);
- *Taasera Licensing LLC v. Check Point Software Technologies Ltd.*, Case No. 2:22cv-00063 (EDTX);
- *Trend Micro Incorporated et al v. Taasera Licensing LLC*, Case No. 3-22-cv-00477 (NDTX);
- *In re: Taasera Licensing LLC*, Patent Litigation, Case No. 2:22-

md03042 (EDTX);

- *Trend Micro Inc. v. Taasera Licensing LLC*, Case No. 2:22-cv-00303 (EDTX);
- *Taasera Licensing LLC v. CrowdStrike, Inc. et al.*, Case No. 6-22-cv-01094 (WDTX);
- *Taasera Licensing LLC v. Fortinet, Inc.*, Case No. 2:22-cv-00415 (EDTX);
- *Taasera Licensing LLC v. Musarubra US, LLC*, Case No. 2:22-cv-00427 (EDTX); and
- *Taasera Licensing LLC v. Crowdstrike, Inc. et al.*, Case No. 2:22-cv-00468 (EDTX).

Petitioner is also aware of the following petitions for *inter partes* review of the ’038 Patent:

- *Palo Alto Networks, Inc. v. Taasera Licensing LLC*, IPR2023-00573

C. Lead And Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)

CrowdStrike provides the following designation of counsel.

Lead Counsel	Backup counsel
W. Karl Renner, Reg. No. 41,265 Fish & Richardson P.C. 60 South Sixth Street, Suite 3200 Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 Email: IPR54971-0010IP1@fr.com	David Holt, Reg. No. 65,161 Fish & Richardson P.C. 60 South Sixth Street, Suite 3200 Minneapolis, MN 55402 Tel: 202-783-5070 Fax: 877-769-7945 PTABInbound@fr.com

D. Service Information

Please address all correspondence and service to the address listed above. Petitioner consents to electronic service by email at IPR54971-0010IP1@fr.com (referencing No. 54971-0010IP1 and cc'ing PTABInbound@fr.com).

Respectfully submitted,

Dated October 24, 2023

/W. Karl Renner/
W. Karl Renner, Reg. No. 41,265
David Holt, Reg. No. 65,161
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

(Control No. IPR2024-00038)

Counsel for Petitioner

CERTIFICATION UNDER 37 CFR § 42.24

Under the provisions of 37 CFR § 42.24(d), the undersigned hereby certifies that the word count for the foregoing Petition for *Inter Partes* Review totals 12,678 words, which is less than the 14,000 allowed under 37 CFR § 42.24.

Dated October 24, 2023

/W. Karl Renner/

W. Karl Renner, Reg. No. 41,265
David Holt, Reg. No. 65,161
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

Counsel for Petitioner

CERTIFICATE OF SERVICE

Pursuant to 37 CFR §§ 42.6(e)(4)(i) *et seq*. and 42.105(b), the undersigned certifies that on October 24, 2023, a complete and entire copy of this Petition for *Inter Partes* Review and all supporting exhibits were provided, by Federal Express, to the Patent Owner by serving the correspondence address of record as follows:

IBM CORPORATION
Intellectual Property Law Department
T.J. Watson Research Center
1101 Kitchawan Road, Route 134, P.O. Box 218
YORKTOWN, NY 10598

/Diana Bradley/
Diana Bradley
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
(858) 678-5667