UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.,
Petitioner,

v.

CENTRIPETAL NETWORKS, INC.,
Patent Owner.

Case No. IPR2018-01512
Patent No. 9,565,213

PATENT OWNER'S PRELIMINARY RESPONSE
UNDER 37 C.F.R. § 42.107

Table of Contents

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

TABLE OF ABBREVIATIONS

Description	Abbreviation
Cisco Systems, Inc.,	"Cisco" or "Petitioner"
Centripetal Networks, Inc.	"Centripetal" or "Patent Owner"
Ex. 1001 – U.S. Patent No. 9,565,213	"the '213 Patent"
Ex. 1004 – Declaration of Dr. Jeffay	"Jeffay Decl."
Ex. 1008 – Cisco ACNS Software Configuration Guide for Centrally Managed Deployments, Release 5.5	"ACNS"
Ex. 1009 – Kjendal et al., U.S. Patent No. 9,172,627	"Kjendal"
Ex. 1011 – An architecture for Differentiated Services	"Diffserv"
"security policy management server"	"SPM"
"packet security gateway"	"PSG"

I. INTRODUCTION

On August 20, 2018, Cisco Systems, Inc., ("Cisco" or "Petitioner") submitted a Petition to institute *inter partes* review ("IPR") of U.S. Patent No. 9,565,213 (Ex. 1001, "the '213 Patent"), challenging claims 1-16. Centripetal Networks, Inc. ("Centripetal" or "Patent Owner") requests that the Board not institute *inter partes* review because Petitioner has not demonstrated a reasonable likelihood that it would prevail in showing unpatentability of any of the challenged claims on the grounds asserted in its Petition, as required under 37 C.F.R. § 42.108(c).

Petitioner's proposed grounds substantively fail to demonstrate a reasonable likelihood that it would prevail in showing unpatentability with respect to the challenged claims. For example, Petitioner did not meet its burden to demonstrate that ACNS, Kjendal, and Diffserv disclose several features of the challenged claims, including:

- (1) "receiving… from the security policy management server, a dynamic security policy that comprises at least one rule specifying application-layer packet-header information and a packet transformation function comprising a packet digest logging function to be performed on packets comprising the application-layer packet-header information" (claim 1) or "receiving… from the security

policy management server, a dynamic security policy that comprises at least one rule specifying packet identification criteria and a packet transformation function comprising a packet digest logging function to be performed on packets corresponding to the packet-identification criteria" (claim 10);

- (2) "identifying, by the packet security gateway, from amongst the packets associated with the network protected by the packet security gateway, and on a packet-by-packet basis, one or more packets comprising the application-layer packet-header information" (claim 1) or "identifying, by the packet security gateway, from amongst the packets associated with the network protected by the packet security gateway, and on a packet-by-packet basis, one or more packets corresponding to the packet-identification criteria" (claims 10); and
- (3) "routing… to a monitoring device each of the one or more packets corresponding to the application-layer packet-header information in response to the performing the packet transformation function" (claim 1) or "routing… to a monitoring device each of the one or more packets corresponding to the packet-identification criteria in response to the performing the packet digest logging function" (claim 10).

Nor has Petitioner met its burden to demonstrate that a person of ordinary skill in the art ("POSA") would have been motivated to make these two and three reference combinations at the time of the invention.

Although there are a variety of reasons that the '213 Patent is not obvious over Petitioner's asserted prior art references, this Preliminary Response focuses on only limited reasons why *inter partes* review should not be instituted. *See Travelocity.com L.P. v. Conos Techs., LLC*, CBM2014-00082, Paper 12 at 10 (PTAB Oct. 16, 2014) ("[N]othing may be gleaned from the Patent Owner's challenge or failure to challenge the grounds of unpatentability for any particular reason."). The deficiencies of the Petition noted herein, however, are sufficient for the Board to find that Petitioner has not met its burden to demonstrate a reasonable likelihood that it would prevail in showing unpatentability of any of the challenged claims.

II. THE '213 PATENT

A. Overview

U.S. Patent No. 9,565,213 discloses "methods and systems for protecting a secured network." Ex. 1001 at Title. The '213 Patent generally describes a network environment 100, which includes Networks A–E 102, 104, 106, 108, and 110. *Id.* at 4:27–30. Network environment 100 may include packet security gateways ("PSGs") 112, 114, 116, and 118, which receive packets and perform

packet transformation functions on the received packets. *Id*. at 4:48–50; 4:66–5:3. Security policy management server ("SPMS") 120 may communicate dynamic security policies to the packet security gateways. *Id*. at 4:53–55; 4:66–5:3.

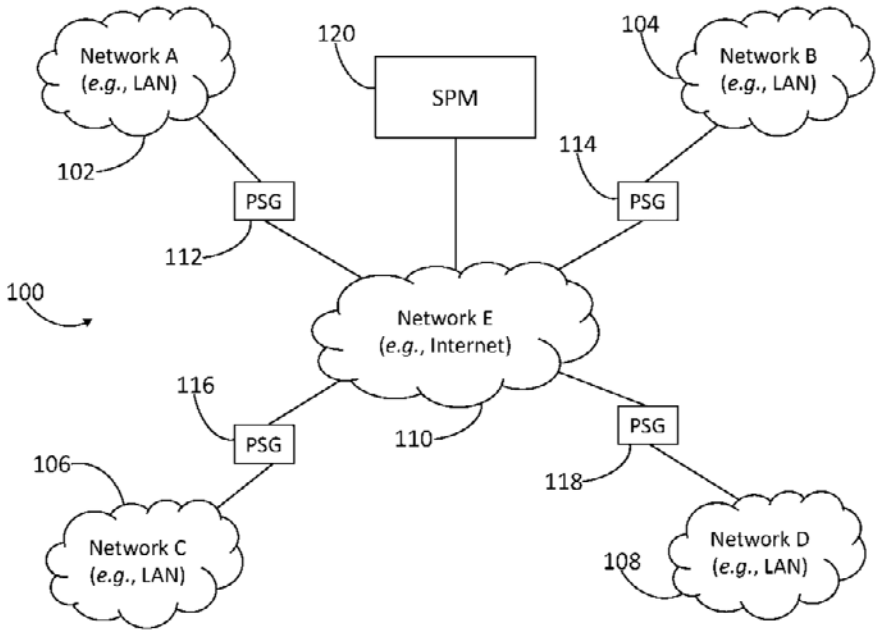


FIG. 1

The exemplary PSGs described in the '213 Patent perform packet transformation functions on the received packets as specified by the dynamic security policy received from the SPMS. *Id*. at 5:21–28. A dynamic security policy may include a number of rules that "may specify criteria and one or more packet transformation functions that should be performed for packets associated with the specified criteria." *Id*. at 7:10–13. "Rules may specify criteria comprising values selected from five-tuple header information and/or values selected from

application-layer header information." *Id.* at 7:67–8:3. As used in the '213 Patent, a packet transformation function is generally described a function that may transform one or more packets from one state to another. *See* § III.E, *infra*.

Upon matching a rule's criteria, a PSG may perform "a packet transformation function configured to route or switch packets… to a network address corresponding to a monitoring device." *Id.* at 11:14–18. In order to effectuate this routing, one embodiment of the '213 Patent provides that "the packet transformation function may be configured to encapsulate such packets (e.g., as described by Internet Engineering Task Force (IETF) Request For Comment (RFC) 2003) with an IP header specifying a network address different from their respective destination addresses." *Id.* at 11:23–26.

The "rules may further specify a packet transformation function that, when applied to a packet that matches such a rule, produces a digest version, or log, of the packet. This packet log (or digest) may contain selected packet information and/or system information (e.g., associated network addresses, ports, protocol types, URIs, arrival times, packet sizes, directions, interface names, media access control (MAC) addresses, matching rule IDs, metadata associated with matching rules, enforced policy names, or the like)." *Id*. at 11:46–54. The packet logs may be used by "[a]wareness application servers [that] may read packet logs and

perform various transformations on the logs to produce awareness information, which may be accessed by client applications." *Id.* at 11:57–60.

B. Challenged Claims

Petitioner challenges claims 1-16 of the '213 Patent, of which claims 1 and 10 are independent. The challenged claims are reproduced in Petition, Appendix A.

III. CLAIM CONSTRUCTION

In an *inter partes* review proceeding, "[a] claim in an unexpired patent that will not expire before a final written decision is issued shall be given its broadest reasonable construction in light of the specification of the patent in which it appears." 37 C.F.R. § 42.100(b); *see also* Office Patent Trial Practice Guide ("Trial Practice Guide"), 77 Fed. Reg. 48756 at 48766 (Aug. 14, 2012); *In re Cuozzo Speed Techs., LLC*, 793 F.3d 1268, 1278 (Fed. Cir. 2015) ("We conclude that Congress implicitly approved the broadest reasonable interpretation standard in enacting the AIA.").

A. "dynamic security policy" (all challenged claims)

The term "dynamic security policy" means "a non-static set of one or more rules, messages, instructions, files, or data structures associated with one or more packets." Petitioner notes that Patent Owner proposed this construction in *Centripetal Networks, Inc., v. Keysight Tech's, Inc., et al.*, 2-17-cv-00383 (E.D.

Va) ("the *Keysight* litigation"). *See* Petition at 14 (citing Ex. 1005, Ex. 1006, and Ex. 1007); *see also* Ex. 2002 at 4–5.

Petitioner's proposed construction, "any rule, message, instruction, file, data structure, or the like that specifies criteria corresponding to one or more packets and identifies a packet transformation function to be performed on packets corresponding to the specified criteria," is incorrect. Petition at 14. *First*, Petitioner's proposed construction improperly reads the term "dynamic" out of the claim. *Second*, Petitioner's proposed construction incorporates its erroneous construction of the term rule into the term "dynamic security policy."

Accordingly, the Board should construe the term "dynamic security policy" to mean "a non-static set of one or more rules, messages, instructions, files, or data structures associated with one or more packets."

B. "rule/rules" (all challenged claims)

The term "rule/rules" means "a condition or set of conditions that when satisfied cause a specific function to occur." This construction matches the district court's construction of the term in the *Keysight* litigation for Centripetal's U.S. Patent No. 9,137,205 (the "'205 Patent"). Ex. 2001 at 21–22.

Petitioner's proposed construction, in which a rule "may specify criteria and one or more packet transformation functions that should be performed for packets associated with the specified criteria," is incorrect ***at least*** because it introduces

criteria and packet transformation functions into the construction. *See* Petition at 14-15.

C. "security policy management server" (all challenged claims)

The term "security policy management server" means "a server configured to manage policies and communicate a dynamic security policy to a packet security." *See* Petition at 15.

D. "packet security gateway" (all challenged claims)

The term "packet security gateway" means "a gateway computer configured to receive packets and perform a packet transformation function on the packets." *See* Petition at 15.

E. "packet transformation function" (all challenged claims)

The term "packet transformation function" means "function that transforms one or more packets from one state to another." Patent Owner proposed this construction in the *Keysight* litigation. *See* Ex. 2002 at 3–5. Petitioner's proposed construction of this term, "an action taken upon a packet," is incorrect for the reasons discussed below. Petition at 16.

First, Petitioner misrepresents representations allegedly made during the *Keysight* litigation. *See* Petition at 16 ("Patent Owner attempted to exclude forwarding and dropping packets from the definition of "packet transformation function" in the Keysight Litigation."). To the contrary, Patent Owner's proposed construction simply did not include the language "such as forward or drop."

Notably, moreover, Patent Owner noted that "[s]ome of the asserted claims [of the '205 Patent] specifically state that the claimed packet transformation function is 'other than forwarding or dropping the packets,' but Defendants intentionally include those excluded functions in its claim term." Ex. 1005 at 5. *Second*, like Defendant's position in the *Keysight* litigation, Petitioner's proposed construction "inappropriately removes any act of 'transformation.'" *Id.*

Accordingly, the term "packet transformation function" should be construed to mean a "function that transforms one or more packets from one state to another."

F. "monitoring device" (all challenged claims)

The term "monitoring device" should be accorded its plain and ordinary meaning, which is "a device configured to monitor packets."

Petitioner's proposed construction of this term, "device configured to copy (or store) packets or data contained within them," is incorrect because it improperly restricts the term "monitoring device" to a specific embodiment described in the specification. See Petition at 17. In particular, the '213 Patent describes that packets may be routed to a monitoring device, which "**may** be configured to copy the packets or data contained within them (e.g., for subsequent review by a law enforcement or national security authority)…." '213 Patent at 11:27–29. Petitioner does not—and could not seriously—allege that this

disclosure of what a monitoring device "may be configured to" do constitutes a definition, disclaimer, or disavowal of claim scope. *See Phillips v. AWH Corp.*, 415 F. 3d 1303, 1316 (Fed. Cir. 2005). Petitioner's construction should therefore be rejected.

IV. THE PETITION IMPROPERLY INCORPORATES ARGUMENTS BY REFERENCE AND FAILS TO MAKE ITS ARGUMENT WITH THE REQUIRED SPECIFICITY

The Petition should be denied because it incorporates vast amounts of information from other documents by reference and fails to explain with the required specificity how that information renders the challenged claims obvious. Under the Board's rules, "[a]rguments must not be incorporated by reference from one document into another document." 37 C.F.R. § 42.6(a)(3). And in an informative opinion on this topic, the Board found that citing "large portions of another document, without sufficient explanation of those portions, amounts to incorporation by reference." *See Cisco Sys., Inc., v. C-Cation Techs., LLC,* IPR2014-00454, Paper 12 at 8 (PTAB Aug. 29, 2014) (informative opinion).

Nevertheless, Petitioner incorporates vast amounts of the Jeffay Declaration ("Jeffay Decl.") into the Petition without providing any explanation for their incorporation. In many cases, the Petition supports broad sweeping arguments that are central to its case and relies exclusively on arguments made in the Jeffay Decl. Throughout the Petition, Petitioner fails to make the underlying evidence available

in the Petition and instead cites to large page ranges of its exhibits, including the Jeffay Decl. This tactic is improper because it fails to make the actual evidence "accessible to the judges" and "amounts to a self-help increase in the length of the brief." *See* Cisco at 10 (informative opinion) (citing *DeSilva v. Dileonardi*, 181 F.3d 865, 866-67 (7th Cir. 1999) ("Incorporation by reference amounts to a self-help increase in the length of the brief, and is a pointless imposition on the court's time. A brief must make all arguments accessible to the judges, rather than ask them to play archeologist with the record.") (modifications omitted)).

Indeed, the Petition is taking the liberty of "a self-help increase in the length of the brief." The Petition is 13,703 words, only 297 words short of the 14,000 word limit provided in 37 C.F.R. § 42.24. The Jeffay Decl., however, is a staggering 34,486 words. The Petition should be denied on this fact alone.

The overwhelming majority of paragraphs in the Petition follow the same format; the Petition makes an assertion relying primarily upon multiple paragraphs of the Jeffay Decl., followed by a short citation to a particular reference that is only tangentially related to the claim element. For example, the following paragraph contains conclusory statements that ACNS discloses the first limitation of claim 1 by parroting the claim language and then that baldly cites to eleven paragraphs of the Jeffay Decl. without support from any of the asserted references:

> "ACNS teaches element [1.1], which requires that packet security gateways (PSGs) receive a dynamic security policy from a security policy management server (SPM Server), and that the dynamic security policy comprises a rule specifying application-layer packet-header information. ***EX1004, ¶¶149-159***. In ACNS, the Content Engines (marked in green, below) represent the claimed PSGs and are associated with a Content Distribution Manager (CDM, marked in yellow) that represents the claimed SPM Server. ***EX1004, ¶150***."

Petition at 26. (emphasis added).

In a further example of Petitioner's conclusory assertions that primarily cite the expansive Jeffay Decl., the Petitioner again parrots a multi-part claim limitation, cites to **19 paragraphs** of the Jeffay Decl. and then cites to tangentially related portions of the asserted reference ACNS under the supporting signal "*see also*."

> "In ACNS, the dynamic security policy includes (1) the set of rules used to configure the operation of the Content Engines (addressed in this claim element) and (2) packet transformation functions to be performed on packets that pass through the Content Engines (addressed below in element [1.2]). ***EX1004, ¶¶149-167***. The dynamic security policy is generated at the CDM based on input by a user. Id., ¶153; see also ***EX1008, 8-24*** (showing step-by-step instructions for generating and updating a policy, which include rules, via the "Content Distribution Manager GUI"); ***EX1008, C-1 – C-27*** (showing command-line interface commands for creating and

> modifying parts of a policy, such as "http add-method" to update a rule identifying a list of allowed HTTP request methods with an additional method)."

Petition at 17. (emphasis added).

Because Petitioner fails to make the underlying evidence available in the Petition itself, it is impossible to gauge whether Petitioner's assertions accurately characterize the underlying information without scouring each page of the many pages and paragraphs cited for any particular conclusory assertion made in the Petition.

This tactic improperly forces Patent Owner and the Board to "play archaeologist with the record" to determine whether or not the conclusory assertion made in the paragraph is actually supported by the record evidence. While the Board in the informative *Cisco* case, cited above, determined that the proper course of action would be to "not consider arguments that are not made in the Petition, but are instead incorporated by reference," the problem is so pervasive in this Petition that it is unclear whether any arguments would remain standing, and outright denial of *inter partes* review is warranted here. *Cisco* at 10. Indeed, to the extent that Petitioner's "arguments" are actually made in the Petition, those arguments so completely torture the underlying evidence as to become unreliable sources for the Board to find a reasonable likelihood that any claim of the '213 Patent is obvious over ACNS, Kjendal, and Diffserv.

Furthermore, Petitioner's tactic of making a conclusory assertion and allegedly supporting that assertion with bare citations to large portions of the record evidence also results in the Petition failing to comply with "the particularity and specificity required of supporting evidence under [the Board's] governing statute and rules," including 37 C.F.R. § 42.104(b)(4*). DirectTV, LLC, v. Qurio Holdings, Inc.*, IPR2015-02006, Paper 6, at 10 (PTAB Apr. 4, 2016). When Petitioner makes conclusory assertions and cites to large portions of a document that allegedly supports that assertion, without making the evidence available in the Petition or explaining how the evidence actually supports the assertion, the Petition cannot satisfy the Board's "governing statute and rules," including 35 U.S.C. § 312(a)(3) and 37 C.F.R. §§ 42.22(a)(2), 42.104(b)(4)–(5). *Id*.

Due to the pervasive and improper incorporation by reference of arguments and evidence not presented in the Petition and Petitioner's failure to meet their burden to state their challenge with "particularity and specificity," Patent Owner requests that the Board decline to institute *inter partes* review of the '213 Patent.

V. SPECIFIC REASONS WHY THE CITED REFERENCES DO NOT INVALIDATE THE CLAIMS, AND WHY *INTER PARTES* REVIEW SHOULD NOT BE INSTITUTED

Petitioner proposes that claims 1–9 of the '213 Patent are rendered obvious by the combination of ACNS in view of Kjendal, and that claims 10–16 are obvious over ACNS in view of Kjendal and in further view of Diffserv. However,

Petitioner has not met its burden to demonstrate that these references, individually or in combination, disclose at least:

(1) receiving a dynamic security policy from a security policy management server,

(2) receiving a dynamic security policy that includes a rule specifying

(a) application-layer packet-header information and

(b) a packet transformation function comprising a packet digest logging function, or

(3) receiving packets associated with a network protected by the packet security gateway,

(4) routing packets corresponding to the application-layer packet-header information to a monitoring device in response to the performing the packet transformation function.

Nor has Petitioner met its burden to demonstrate that a POSA would have combined those references to arrive at the claims of the '213 Patent.

A. ACNS in View of Kjendal Does Not Render Obvious Claims 1–9

The Board should decline to institute *inter partes* review at least because ACNS in view of Kjendal does not render challenged claims 1–9 obvious under 35 U.S.C. § 103.

1. Petitioner Has Not Demonstrated that ACNS in View of Kjendal Discloses Receiving a Dynamic Security Policy From a Security Policy Management Server (claims 1–9)

Contrary to Petitioner's contention, ACNS and Kjendal, taken alone or in combination, fail to disclose "receiving… from the security policy management server, a dynamic security policy that comprises at least one rule specifying application-layer packet-header information and a packet transformation function comprising a packet digest logging function comprising a packet digest logging function to be performed on packets comprising the application-layer packet-header information." Petition at 25–30. In fact, ACNS and Kjendal are so inconsistent with the '213 Patent that Petitioner primarily relies upon the Jeffay Decl.—not ACNS or Kjendal—to assert this limitation is met. As explained below, this limitation is not met by ACNS in view of Kjendal.

The challenged claims recite PSGs that receive dynamic security policies from an SPMS. The ACNS reference, however, does not teach or suggest a SPMS. In contract, ACNS teaches a Content Distribution Manager for providing "centralized content and device management." EX1008 at 38. The Content Distribution Manager is not concerned with network security and does not provide the claimed dynamic security policies to the Content Engines, which Petitioner alleges correspond to the claimed PSGs. Ex. 1008 at 38. As shown below, the

Content Distribution Manager is not described in ACNS as being concerned with security:

> "The Primary role of a Content Distribution Manager is to perform centralized content and device management. In the ACNS 5.5 network, the Content Distribution Manager manages both content acquisition and distribution and also manages policy settings and configurations on individual Content Engines. Through the Content Distribution Manager GUI, the network administrator can specify what content is to be distributed and to whom. The Content Distribution Manager also allows the administrator to monitor network nodes and apply changes, such as software upgrades, to groupings of nodes from a central location."

Id.

Furthermore, the Content Engines do not receive any policies from the Content Distribution Manager. Rather, the Content Distribution Manager "manages both content acquisition and distribution and also **manages** policy settings and configurations on individual Content Engines." *Id.* (emphasis added). Thus, while the Content Distribution Manager does manage individual policy settings for policies pre-existing on the Content Engines, the Content Engines **do not** receive their policies from the Content Distribution Manager. *Id.* Instead, the Content Distribution Manager is merely capable of managing an existing policy already installed on a Content Engine. *Id.* ("[T]he Content Distribution

Manager…manages policy setting and configuration."). ACNS simply does not teach that the Content Distribution Manager sends any **policy** to the Content Engine.

Petitioner's allegation that ACNS discloses this claim element is facially deficient. While Petitioner alleges that the dynamic security policy is "the set of rules used to configure the operation of the Content Engines," it mischaracterizes the disclosure of ACNS to suggest that such policies are generated on the CDM when they are not. *See* Petition at 27 (asserting that "[t]he dynamic security policy is **generated** at the CDM based on input by a user") (emphasis added).

In an attempt to support this proposition, Petitioner first cites to the declaration of its expert, Dr. Jeffay. Petition at 27 (citing Jeffay Decl, ¶ 153). However, Dr. Jeffay cites no evidence that the **policies** enforced by the Content Engines are generated at the CDM. Rather, Dr. Jeffay only cites to a portion of ACNS that involves using the CDM to add a rule to or modify a rule of an existing Content Engine policy. *See* Jeffay Decl., ¶ 153(citing Ex. 1008 at 8-23–8-24). To wit, ACNS discloses "Adding or Modifying **Additional** HTTP Request Methods for the Content Engine," not generating and/or sending a policy to a Content Engine. Ex. 1008 at p. 342 (emphasis added).

Adding or modifying a request method involves adding one HTTP request method to a plurality of request methods already configured on the Content Engine

or modifying one of those already configured request methods. *See* Ex. 1008 at p. 342 ("Step 6: In the Method Name field, enter the name of the HTTP request method to be added to the list of supported methods."). To the extent that the Petitioner alleges that the set of request methods corresponds to the claimed "dynamic security policy," ACNS discloses adding a new rule to a policy that pre-exists on the Content Engine rather than a Content Engine receiving the policy itself from the CDM.

The Petition's second example of a "dynamic security policy" suffers the same deficiency. In particular, ACNS teaches adding or modifying a rule of a pre-existing policy located on the Content Engine using a command line interface (CLI). Ex. 1008 at p. 895. Petitioner relies upon Table C-1 as allegedly teaching the dynamic security policy provisioned to the Content Engine by the Content Distribution Manager. Petition at 27. However, Table C-1 only shows a table of commands that may be used to **modify** a setting or rule on the Content Engine. Ex. 1008 at p. 895-920. To the extent that Petitioner alleges that the commands when viewed together are a dynamic security policy, this limitation of claim 1 still would not be met because these commands are not provisioned to the Content Engine from the Content Distribution Manager as a policy. Instead, the commands adjust settings that pre-exist on the Content Engine, and each setting can be adjusted using the CLI. *Id*. (describing list of CLI commands for the Content Engine).

For at least these reasons, ACNS in view of Kjendal does not teach or suggest "receiving… from the security policy management server, a dynamic security policy that comprises at least one rule specifying application-layer packet-header information and a packet transformation function comprising a packet digest logging function comprising a packet digest logging function to be performed on packets comprising the application-layer packet-header information," as required by claims 1-9.

2. Petitioner Has Not Demonstrated that ACNS in View of Kjendal Discloses Receiving a Dynamic Security Policy Comprising a Rule Specifying a Packet Digest Logging Function

Petitioner improperly divorces the claimed "dynamic security policy that comprises a rule specifying" from "a packet transformation function comprising a packet digest logging function to be performed on packets comprising the application-layer packet-header information" in sections [1.1] and [1.2] of the Petition, respectively. Petitioner then improperly attempts to prove that each half of the limitation is obvious without giving weight to the other half of the claim limitation in its analysis.

As shown below, the claim element Petitioner labels as [1.2] is part of the claimed "dynamic security policy comprising at least one rule specifying" and cannot be divorced from the claimed dynamic security policy for the purpose of

asserting unpatentability. Shown below is claim 1 with formatting inserted to show the two parts to a dynamic security policy in the '213 Patent:

> receiving ... a dynamic security policy that comprises at least one rule specifying
>
> **[1]** application-layer packet-header information and
>
> **[2]** a packet transformation function comprising a packet digest logging function to be performed on packets comprising the application-layer packet-header information;

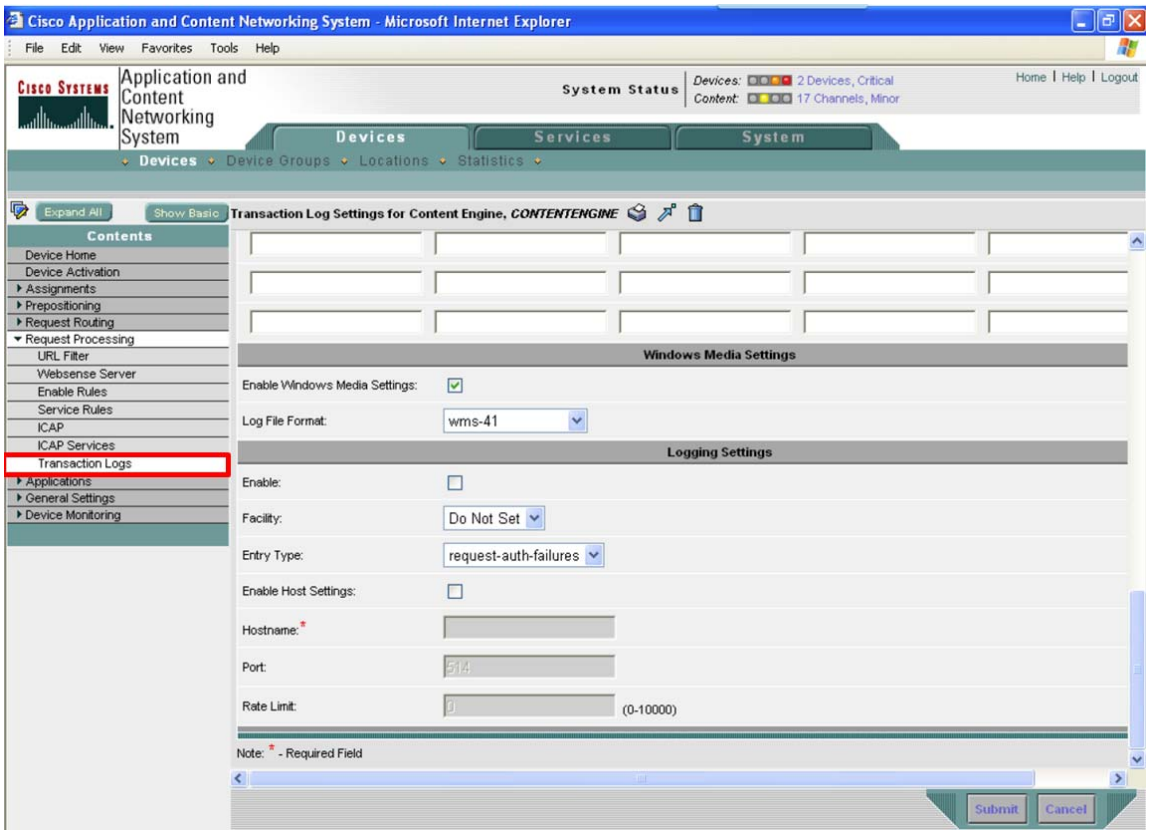
'213 Patent at claim 1 (formatting added, and annotations added in bold text).

Petitioner asserts that ACNS' teaching of transaction logging renders obvious the claimed "packet digest logging function." However, it is not enough for Petitioner to merely show the presence of transaction logging to demonstrate that "receiving ... a dynamic security policy that comprises at least one rule specifying... a packet transformation function comprising a packet digest logging function to be performed on packets comprising the application-layer packet-header information" is obvious in light of ACNS and Kjendal. Indeed, Petitioner attempts demonstrate that a "packet digest logging function" is obvious without demonstrating that the alleged "packet digest logging function" is part of a "dynamic security policy." Petition at 30-37.

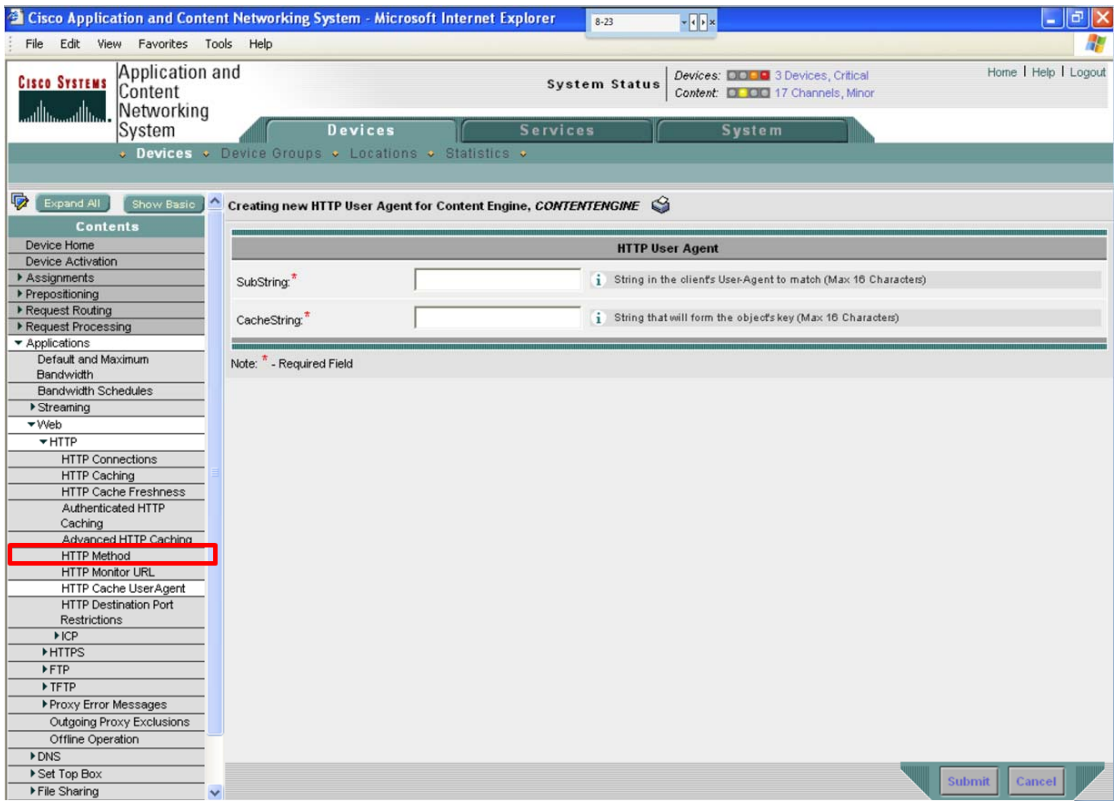
Petitioner fails to make any showing that its proposed combination of ACNS in view of Kjendal discloses "receiving… a dynamic security policy that comprises

at least one rule specifying… a packet transformation function comprising a packet digest logging function to be performed on packets comprising the application-layer packet-header information," in dereliction of their obligation under 37 C.F.R. § 42.104(b)(4). *See* Petition at 30-37 (discussing Element [1.2] and failing to make a *prima facie* case in that the alleged "packet digest logging function" of ACNS is part of a dynamic security policy).

Petitioner alleges that the transaction logging functionality of ACNS maps to the "packet digest function" of '213 Patent claims. *See* Petition at 32. Specifically, Petitioner point to Ex. 1008 at p. 717-718 (ACNS at 19-21–19-22) ("About Specifying the Transaction Log Entry Type When Logging to a Remote Syslog Host."). However, the ACNS' Transaction Logs are unrelated to the HTTP Method policy that Petitioner alleges is received as a dynamic security policy from the Content Distribution Manager. As shown in the GUIs below, ACNS' transaction logs and HTTP methods are completely unrelated. *Compare*

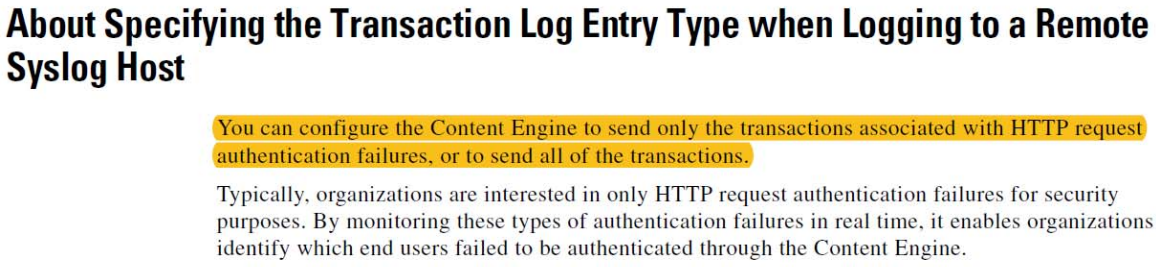


Ex. 1008 at p. 713 (showing ACNS transaction logs GUI) *with*



Ex. 1008 at p. 343 (showing ACNS HTTP Method GUI).

Indeed, the transaction logging functionality of ACNS that Petitioner alleges teaches the "packet-digest logging function" is not applied to packets particularly identified to have "application-layer packet header information." Rather, as shown below, ACNS specifically states that it either logs **every** HTTP request or only those HTTP requests for which user **authentication** had failed (also shown in above proof).



About Specifying the Transaction Log Entry Type when Logging to a Remote Syslog Host

You can configure the Content Engine to send only the transactions associated with HTTP request authentication failures, or to send all of the transactions.

Typically, organizations are interested in only HTTP request authentication failures for security purposes. By monitoring these types of authentication failures in real time, it enables organizations to identify which end users failed to be authenticated through the Content Engine.

EX1008 at p. 717. Accordingly, ACNS does not teach or suggest that the alleged "packet digest logging function" is to be performed on packets having the specified "application-layer packet-header information" or that it is part of what Petitioner contends is the dynamic security policy received from the CDM.

Indeed, Petitioner acknowledges that "ACNS does not explicitly disclose that the logging function can be applied to log packets based on application-layer packet-header information identified by the HTTP request or ICAP rules." Petition at 35. Petitioner instead relies on "Kjendal teach[ing] that packets may be mirrored (i.e. sent to a network logger) based on dynamic rules specifying application-layer packet header information, such as identification of specific application types." *Id.* However, while Kjendal does disclose that one use of its technology is to mirror copies of packets to a network logger, mirroring a packet is **not** a packet digest logging function, regardless of where the mirrored packet is sent. Indeed, Kjendal's rules do not control what occurs at the network logger, let alone specify that the network logger carry out a specified packet digest logging function. Kjendal at 10:46–49.

That is, simply sending a copy of a packet to a device called a "network logger" is not a packet digest logging function, as claimed, which requires *inter alia* "identifying a subset of information," "generating… a record comprising the subset of information," and "reformatting… the subset of information." *See* '213 Patent at claims 1 and 10. Accordingly, even taken in combination, ACNS and Kjendal fail to disclose receiving a dynamic security policy that includes a rule specifying (1) application-layer packet-header information and (2) a packet digest logging function to be performed upon matching application-layer packet-header information.

For at least these reasons, ACNS in view of Kjendal does not teach or suggest "receiving… a dynamic security policy that comprises at least one rule specifying… a packet transformation function comprising a packet digest logging function to be performed on packets comprising the application-layer packet-header information," as required by claims 1-9.

3. Petitioner Has Not Demonstrated that ACNS in View of Kjendal Discloses Receiving Packets Associated With a Network Protected by the Packet Security Gateway

Petitioner purports to map the Content Engine of ACNS to the "packet security gateways" of the '213 Patent and asserts that these Content Engines protect a network. Petitioner's argument relies on one oblique reference in ACNS that states the Content Engine protects a network. Petition at 38. However,

Petitioner has not demonstrated that these Content Engines protect any network using a dynamic security policy. At best, the policy Petitioner points to performs access control techniques unrelated to network security. EX1008 at p. 45 (disclosing that the Content Engines "control web access from end users to implement corporate policies regarding work environment and system security."). For example, the ACNS web access controls include preventing unauthorized web requests from leaving the corporate network (e.g. preventing requests to social media website, entertainment website, etc.). *Id*. Accordingly, there is no teaching in ACNS that the Content Engine protects the network using a dynamic security policy.

Petitioner additionally relies on ACNS' disclosure of preventing viruses, but that functionality is not disclosed to be carried out by the Content Engine, which was mapped the claimed PSG. Petition at 38. Rather, it is done by an ICAP server in communication with the Content Engine. Ex. 1008 at p. 609 ("ICAP specifies how a Content Engine, acting as an HTTP proxy server, can **communicate with an external device that is acting as an ICAP server, which filters and adapts the requested content**.").

For at least these reasons, ACNS in view of Kjendal does not teach or suggest "identifying, by the packet security gateway, from amongst the packets associated with the network protected by the packet security gateway, and on a

packet-by-packet basis, one or more packets comprising the application-layer packet-header information," as required by claims 1-9.

4. Petitioner Has Not Demonstrated that ACNS in View of Kjendal Discloses Routing Packets Corresponding to the Packet-Identification Criteria to a Monitoring Device in Response to Performing the Packet Digest Logging Function

Petitioner cites Kjendal alone for this claim element. Petition at 45-47. However, Kjendal does not disclose routing packets corresponding to the application-layer packet-header information to a monitoring device. Rather, Kjendal describes "**mirroring** of the one or more packets or portions of packets to a destination other than the original intended destination." Kjendal at 7:49-51 (emphasis added). The mirroring involves copying packets without disrupting the original data flow. *Id*. at 7:60-64 ("Frames of flows of traffic from any packet forwarding device can be mirrored without disturbing the normal routing of the messages and maximizing the usage of network bandwidth and the usage of other devices of the network, including IDSs."). Accordingly, the "packets" that allegedly match that rule are not routed to a monitoring device because their flow is not disturbed. *Id*.

Kjendal also describes performing this mirroring **before** identifying any application data, let alone application-layer packet-header information. Kjendal at 7:43-49 ("An aspect of the present invention is the forwarding of one or more frames contained in packets or one or more portions of frames in packets of a flow

or at the initiation of a session to the application identification engine of one or more devices of the network infrastructure for the purpose of determining the application associated with the flow/session being established.").

For at least these reasons, ACNS in view of Kjendal does not teach or suggest "routing… to a monitoring device each of the one or more packets corresponding to the application-layer packet-header information in response to the performing the packet transformation function," as required by claims 1-9.

5. Petitioner Has Not Demonstrated That It Would Have Been Obvious To Combine ACNS and Kjendal

ACNS and Kjendal are disparate systems that one of skill in the art would not have been motivated to combine. Petitioner offers merely conclusory statements that a POSA would be motivated to combine ACNS and Kjendal. Petition at 24-25. However, the law is clear, "Petitioner must show some reason why a person of ordinary skill in the art would have thought to combine particular available elements of knowledge, as evidenced by the prior art, to reach the claimed invention." *Heart Failure Techs., LLC v. CardioKinetix, Inc.*, IPR2013-00183, Paper No. 12 at 9 (P.T.A.B. July 31, 2013)(citing *KSR Int'l Co. v. Teleflex, Inc.*, 550 U.S. 398, 418 (2007))(original emphasis removed, emphasis added).

First, Petitioner alleges that a POSA would be motivated to combine the "packet-mirroring teachings" of Kjendal with the teachings of ACNS because "port-mirroring was well-known at the time of the alleged invention, and that such

systems were routinely deployed on Cisco router systems." *Id.* at 24. Petitioner generally alleges that "[t]his teaching of monitoring by ACNS would prompt a POSA to combine its teaching with related art, such as Kjendal, which specifically teaches how to monitor packets through mirroring." *Id.* at 25.

Petitioner, however, provides no specific reasons why a POSA would be motivated to add "port-mirroring" to the ACNS system other than that it was well-known. *Id.* at 24-25. However, whether or not port-mirroring was well-known in the art is not a reason that a POSA would implemented port-mirroring within ACNS. *See KSR Intern. Co. v. Teleflex Inc.*, 550 U.S. 398, 418 ("[I]t can be important to identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed new invention does ... because inventions in most, if not all, instances rely upon building blocks long since uncovered, and claimed discoveries almost of necessity will be combinations of what, in some sense, is already known.").

In fact, there is no motivation to combine ACNS and Kjendal because a POSA would not be motivated to modify ACNS with the packet-mirroring functionality of Kjendal. Petitioner's argument relies on a mischaracterization of Kjendal, namely that "Kjendal discloses a system where application-layer packet-header information is used to determine what should be logged." Petition at 31. Kjendal, which only discloses determining **whether** and **where** a packet should be

mirrored, teaches no such thing. *See* Kjendal at 29:13–17 (disclosing mirroring one or more packets based on selected criteria); 30:14–16 (disclosing using application layer as a first criteria); *id.* at 29:67–30:1 (disclosing the first criteria as being "based on a field or selected fields in the packet"). Thus, while Kjendal does disclose that one device that might receive a mirrored packet is "network logger," there is no evidence that Kjendal's rules control what occurs at the network logger, let alone that the rules specify a packet digest logging function to be performed upon matching application-layer packet-header information.

Furthermore, a POSA would not be motivated to modify this functionality with "packet-mirroring" described in Kjendal because ACNS does not require packet-mirroring to view network traffic at the Content Engine—it already logs packets without the need to perform packet-mirroring. ACNS provides logging functionality that "allow[s] administrators to view the traffic that has passed through the Content Engine." Ex. 1008 at p. 697. Kjendal provides the functionality of mirroring traffic based on specific criteria. However, ACNS describes using criteria to perform functions such as adding crawl tasks to a channel, searching for media, filtering HTTP certificate groups. *See* Ex. 1008 at p. 217, 302, 350.

ACNS does not describe a need to mirror-traffic based on criteria, and Petitioner does not identify any benefit to be gained by using Kjendal's mirroring

techniques. Accordingly, the Petition should be denied because there is insufficient evidence that a POSA would have combined ACNS with Kjendal to reach the claims of the '213 Patent.

B. ACNS in view of Kjendal and in further view of Diffserv Do Not Render Obvious Claims 10-16

The Board should decline to institute *inter partes* review at least because ACNS in view of Kjendal and in further view of Diffserv do not render challenged claims 10-16 obvious under 35 U.S.C. § 103.

1. Petitioner Has Not Demonstrated that ACNS in View of Diffserv Receiving a Dynamic Security Policy From a Security Policy Management Server, Where the Dynamic Security Policy Includes a Rule Specifying a Packet Digest Logging Function (claim 10)

As discussed above, Petitioner has not met its burden to demonstrate that ACNS in view of Kjendal discloses "receiving… from the security policy management server, a dynamic security policy that comprises at least one rule specifying packet identification criteria and a packet transformation function comprising a packet digest logging function to be performed on packets corresponding to the packet-identification criteria." *See* § V.A., *supra*. Petitioner relies on the same deficient arguments for its application of ACNS in view of Diffserv to claim 10. *See* Petition at 62-63 ("Claim element [10.1] is similar to element [1.1] except that element [10.1] more broadly recites that the rule includes packet-identification criteria, rather than application-layer packet header

information…Therefore, any teaching that satisfies [1.1] also satisfies [10.1] and all discussion of ACNS for [1.1] is incorporated here.").

Petitioner's arguments with respect to claim 10 fail for the same reasons that it fails for claim 1—namely, that ACNS does not teach or suggest a security policy management server that provisions packet security gateways with the claimed dynamic security policy. *See* § V.A.1, *supra*.

Petitioner also argues that Diffserv teaches "classifier rules [that] include packet identification criteria." Petition at 63. Diffserv, however, does not cure the deficiencies of ACNS because Diffserv does not teach or suggest that the classifier rules are part of a dynamic security policy or that they are provisioned from a security policy management server to a packet security gateway.

2. The combination of ACNS in view of Kjendal in further view of Diffserv fail to teach or suggest "identifying, by the packet security gateway, from amongst the packets associated with the network protected by the packet security gateway, and on a packet-by-packet basis, one or more packets corresponding to the packet-identification criteria" (claims 10-16)

As discussed above, Petitioner has not met its burden to demonstrate that ACNS in view of Kjendal and Diffserv disclose "identifying, by the packet security gateway, from amongst the packets associated with the network protected by the packet security gateway, and on a packet-by-packet basis, one or more packets corresponding to the packet-identification criteria," as recited in independent claim 10." See § V.A.3, *supra*. Petitioner relies on the same deficient

arguments for its application of Kapoor and Kjendal to independent claim 10. See Petition at 65 ("This element is identical to element [1.3] regarding gateways receiving packets, and analysis of that element is incorporated here"). Accordingly, Petitioner's arguments for this element fail for the same reasons as in claim 1.

3. The combination of ACNS in view of Kjendal in further view of Diffserv fail to teach or suggest "routing, by the packet security gateway and on a packet-by-packet basis, to a monitoring device each of the one or more packets corresponding to the packet-identification criteria in response to the performing the packet digest logging function." (claims 10-16)

As discussed above, Petitioner has not met its burden to demonstrate that ACNS in view of Kjendal and Diffserv disclose "routing, by the packet security gateway and on a packet-by-packet basis, to a monitoring device each of the one or more packets corresponding to the packet-identification criteria in response to the performing the packet digest logging function," as recited in independent claim 1." See § V.A.4, supra. Petitioner relies on the same deficient arguments for its application of Kapoor and Kjendal to independent claim 10. See Petition at 68-69 ("This element is very similar to element [1.9], except for how the packets are identified as addressed for element [10.5], and the analysis of elements [1.9] and [10.5] is incorporated by reference to show this element is obvious"). Accordingly, Petitioner's arguments for this element fail for the same reasons as in claim 1.

VI. CONCLUSION

Petitioner has not established a reasonable likelihood that it will prevail in establishing that claims 1–16 of the '213 Patent are invalid. Centripetal accordingly requests that the Board deny institution of *inter partes* review of the '213 Patent.

Respectfully submitted,

Dated: December 21, 2018

/James Hannah/

James Hannah (Reg. No. 56,369)
Michael Lee (Reg. No. 63,941)
Kramer Levin Naftalis & Frankel LLP
990 Marsh Road
Menlo Park, CA 94025
Tel: 650.752.1700 Fax: 212.715.8000

Jeffrey H. Price (Reg. No. 69,141)
Kramer Levin Naftalis & Frankel LLP
1177 Avenue of the Americas
New York, NY 10036
Tel: 212.715.7502 Fax: 212.715.8302

Bradley C. Wright (Reg. No. 38,061)
Banner & Witcoff, Ltd.
1100 13th Street NW, Suite 1200,
Washington, DC 20005.
Tel: 202.824.3160. Fax: 202.824.3000.
Email: bwright@bannerwitcoff.com.

(Case No. IPR2018-01512) *Attorneys for Patent Owner*

CISCO SYSTEMS, INC.,
v.
CENTRIPETAL NETWORKS, INC.,

Case IPR2018-01512
Patent 9,565,213

PATENT OWNER'S EXHIBIT LIST

Exhibit-2001 Opinion and Order re Claim Construction, *Centripetal Networks, Inc., v. Keysight Tech's, Inc., et al*., No. 2:17-cv-00383 (Dkt. 484).

Exhibit-2002 Amended Joint Claim Construction Statement, Exhibit 2, *Centripetal Networks, Inc., v. Keysight Tech's, Inc., et al*., No. 2:17-cv-00383 (Dkt. 244-2).

CERTIFICATE OF COMPLIANCE WITH 37 C.F.R. § 42.24

This paper complies with the type-volume limitation of 37 C.F.R. § 42.24. The paper includes 6,943 words, excluding the parts of the paper exempted by § 42.24(a).

This paper also complies with the typeface requirements of 37 C.F.R. § 42.6(a)(ii) and the type style requirements of § 42.6(a)(iii)&(iv).

/James Hannah/

James Hannah (Reg. No. 56,369)
Kramer Levin Naftalis & Frankel LLP
990 Marsh Road,
Menlo Park, CA 94025
(650) 752-1700

CERTIFICATE OF SERVICE

The undersigned certifies, in accordance with 37 C.F.R. § 42.6(e), that service was made on the Petitioner as detailed below.

Date of service December 21, 2018

Manner of service Electronic Mail

(dmcdonald@merchantgould.com;
jblake@merchantgould.com;
kott@merchantgould.com;
cdavis@merchantgould.com)

Documents served PATENT OWNER'S PRELIMINARY RESPONSE

Persons Served Daniel W. McDonald
Jeffrey D. Blake
Kathleen E. Ott
Christopher C. Davis

/James Hannah/
James Hannah
Registration No. 56,369
Counsel for Patent Owner