

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

NORMSHIELD INC. d/b/a BLACK KITE INC.,

Petitioners,

v.

BITSIGHT TECHNOLOGIES, INC.,

Patent Owner.

Case No. IPR2025-00276

U.S. Patent No. 11,777,976

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 11,777,976**

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION	1
II. STANDING.....	2
III. GROUNDS.....	2
IV. POSITA.....	2
V. BACKGROUND	2
A. Technical Background (EX1003, ¶¶50-67)	2
B. Public Availability	14
1. McNab.....	14
2. Internet Archive Pages.....	14
3. Public Videos.....	15
C. '976 patent.....	17
1. Prosecution History (EX1003, ¶¶70-72)	18
VI. CLAIM CONSTRUCTION	18
VII. GROUNDS.....	18
A. Ground 1: Tippet	18
1. Claim 1	18
(a) 1[pre]: A method for determining a security rating of an entity, the method comprising:	18
(b) 1[a]: determining an internal security rating comprising:.....	19
(c) 1[b]: obtaining data indicative of internal security from a plurality of internal data sources;	20
(d) 1[c]: extracting a plurality of internal security features from the obtained data;	22
(e) 1[d]: applying a respective transformation function to each of the plurality of internal security features to determine a first plurality of transformed features; and.....	22

(f)	1[e]: combining the first plurality of transformed features to form the internal security rating;.....	23
(g)	1[f]: determining an external security rating comprising:.....	24
(h)	1[g]: obtaining data indicative of external security from a plurality of external data sources;	25
(i)	1[h]: extracting a plurality of external security features from the obtained data;	27
(j)	1[i]: applying a respective transformation function to each of the plurality of external security features to determine a second plurality of transformed features; and.....	27
(k)	1[j]: combining the second plurality of transformed features to form the external security rating; and.....	28
(l)	1[k]: providing, via a reporting facility, a composite security rating for the entity based on the internal security rating and the external security rating, wherein at least one of the internal security features or the external security features indicates malicious activity associated with an IP address of the entity.....	29
2.	Claim 2: The method of claim 1, further comprising: determining the composite security rating based on a weighted combination of the internal security rating and the external security rating.	31
3.	Claim 4: The method of claim 1, wherein at least one of the internal security features or the external security features comprise at least one of: a number of remotely exploitable vulnerabilities of the entity; a number of security incidents; or a number of vulnerable versions of software of the entity.	31
4.	Claim 5: The method of claim 1, wherein each respective transformation function is a normalization of the respective feature, and further comprising: when the normalization is applied to two or more of the internal security features or the external security features, summing the normalized features.....	32

5.	Claim 6: The method of claim 1, wherein determining the internal security rating further comprises weighting the first plurality of transformed features.	33
6.	Claim 7: The method of claim 1, wherein combining the first plurality of transformed features comprises: summing the first plurality of transformed features; and normalizing the summed features by a set of normalization factors.	34
7.	Claim 8: The method of claim 1, wherein combining the second plurality of transformed features comprises: summing the second plurality of transformed features; and normalizing the summed features by a set of normalization factors.	35
8.	Claim 9	37
	(a) 9[pre]: A system for determining a security rating of an entity, the system comprising:	37
	(b) 9[a]: one or more computer systems programmed to perform operations comprising:	37
	(c) 9[b]: determining an internal security rating comprising:	37
	(d) 9[c]: obtaining data indicative of internal security from a plurality of internal data sources;	38
	(e) 9[d]: extracting a plurality of internal security features from the obtained data;	38
	(f) 9[e]: applying a transformation function to each of the plurality of internal security features; and	38
	(g) 9[f]: combining the transformed features to form the internal security rating;	38
	(h) 9[g]: determining an external security rating comprising:	38
	(i) 9[h]: obtaining data indicative of external security from a plurality of external data sources;	38
	(j) 9[i]: extracting a plurality of external security features from the obtained data;	38
	(k) 9[j]: applying a transformation function to each of the plurality of external security features; and	38

- (l) 9[k]: combining the transformed features to form the external security rating; and 39
 - (m) 9[l]: providing, via a reporting facility, a composite security rating for the entity based on the internal security rating and the external security rating, wherein at least one of the internal security features or the external security features indicates malicious activity associated with an IP address of the entity.....39
- 9. Claim 10: The system of claim 9, wherein the one or more computer systems are further programmed to perform operations comprising: determining the composite security rating based on a weighted combination of the internal security rating and the external security rating. 39
- 10. Claim 12: The system of claim 9, wherein the internal security features and the external security features comprise at least one of: a number of remotely exploitable vulnerabilities of the entity; a number of security incidents; or a number of vulnerable versions of software of the entity.....39
- 11. Claim 13: The system of claim 9, wherein each respective transformation function is a normalization of the respective feature, and wherein the one or more computer systems are further programmed to perform operations comprising: when the normalization is applied to two or more of the internal security features or the external security features, summing the normalized features. 40
- 12. Claim 14: The system of claim 9, wherein determining the internal security rating further comprises weighting the first plurality of transformed features. 40
- 13. Claim 15: The system of claim 1, wherein combining the first plurality of transformed features further comprises: summing the first plurality of transformed features; and normalizing the summed features by a set of normalization factors. 40
- 14. Claim 16: The system of claim 9, wherein combining the second plurality of transformed features further comprises: summing the second plurality of transformed

features; and normalizing the summed features by a set of normalization factors.	41
B. Ground 2: Tippet, McGovern.....	41
1. Motivation to Combine	41
2. Claim 3: The method of claim 1, wherein the plurality of internal data sources comprises: vulnerability scan data of the entity; data indicating firewall rules of the entity; data from security incident reports corresponding to the entity; data indicative of computer network configurations of the entity; data indicative of software inventory of the entity; data indicative of security policies of the entity; data indicative of security controls of the entity; and data indicative of user behavior corresponding to the entity.	45
3. Claim 11: The system of claim 9, wherein the plurality of internal data sources comprises: vulnerability scan data of the entity; data indicating firewall rules of the entity; data from security incident reports corresponding to the entity; data indicative of computer network configurations of the entity; data indicative of software inventory of the entity; data indicative of security policies of the entity; data indicative of security controls of the entity; and data indicative of user behavior corresponding to the entity.	49
VIII. MANDATORY NOTICES AND FEES	49
A. Real Party-In-Interest.....	49
B. Related Matters.....	50
C. Counsel and Service Information	50
D. Payment of Fees.....	51

EXHIBIT LIST

Ex.	Description
1001	U.S. Patent No. 11,777,976 (“’976 patent”)
1002	Prosecution History for U.S. Patent No. 11,777,976
1003	Declaration of Dr. Kevin Almeroth
1004	<i>Curriculum Vitae</i> of Kevin Almeroth Ph.D.
1005	McNab, “Network Security Assessment,” O’Reilly Media, Inc. (2008) (prior art under at least § 102(b))
1006	U.S. Pat. Pub. No. 2005/0278786 A1 (“Tippett”) (prior art under at least § 102(b))
1007	U.S. Pat. Pub. No. 2009/0024663 A1 (“McGovern”) (prior art under at least §§ 102(b))
1008-1012	Intentionally Left Blank
1013	Declaration of Nathaniel Frank-White and accompanying exhibits
1014	Declaration of Sylvia Hall-Ellis, Ph.D. and accompanying exhibits
1015	Matta Security Limited, “An Introduction to Internet Attack & Penetration,” available at https://web.archive.org/web/20070202020317/http://www.trustmatta.com/downloads/pdf/Matta_Attack_and_Penetration_Introduction.pdf
1016	Stoneburgner, et al., “Risk Management Guide for Information Technology Systems,” NIST, available at https://www.archives.gov/files/era/recompete/sp800-30.pdf
1017	Moore & Valsmith, et al., “Tactical Exploitation,” available at https://web.archive.org/web/20100208161237/https://www.blackhat.com/presentations/bh-usa-

	07/Moore_and_Valsmith/Whitepaper/bh-usa-07-moore_and_valsmith-WP.pdf
1018	Chris Gates, “New School Information Gathering” (2008) available at https://www.carnal0wnage.com/papers/17_Gates.pdf
1019	Chis Gates, “Toorcon X Gates: New School Information Gathering,” available at http://vimeo.com/2745624
1020	Chis Gates, “Toorcon X Gates: New School Information Gathering,” available at https://web.archive.org/web/20090302045813/https://vimeo.com/2745624
1021	Social-Engineer, LLC, “Social Engineering Using Maltego,” available at https://www.youtube.com/watch?v=qiv4-wy3mxo
1022-1028	Intentionally Left Blank
1029	August 29, 2024 Email from Melissa Nezhnik
1030	Metadata for YouTube video ID qiv4-wy3mxo
1031	Relevant screen captures of Exhibit 1021

LIST OF CHALLENGED CLAIMS

Claim	Limitation
1[pre]	A method for determining a security rating of an entity, the method comprising:
1[a]	determining an internal security rating comprising:
1[b]	obtaining data indicative of internal security from a plurality of internal data sources;
1[c]	extracting a plurality of internal security features from the obtained data;
1[d]	applying a respective transformation function to each of the plurality of internal security features to determine a first plurality of transformed features; and
1[e]	combining the first plurality of transformed features to form the internal security rating;
1[f]	determining an external security rating comprising:
1[g]	obtaining data indicative of external security from a plurality of external data sources;
1[h]	extracting a plurality of external security features from the obtained data;
1[i]	applying a respective transformation function to each of the plurality of external security features to determine a second plurality of transformed features; and
1[j]	combining the second plurality of transformed features to form the external security rating; and
1[k]	providing, via a reporting facility, a composite security rating for the entity based on the internal security rating and the external security rating, wherein at least one of the internal security features or the external security features indicates malicious activity associated with an IP address of the entity.

Claim	Limitation
2	The method of claim 1, further comprising: determining the composite security rating based on a weighted combination of the internal security rating and the external security rating.
3	The method of claim 1, wherein the plurality of internal data sources comprises: vulnerability scan data of the entity; data indicating firewall rules of the entity; data from security incident reports corresponding to the entity; data indicative of computer network configurations of the entity; data indicative of software inventory of the entity; data indicative of security policies of the entity; data indicative of security controls of the entity; and data indicative of user behavior corresponding to the entity.
4	The method of claim 1, wherein at least one of the internal security features or the external security features comprise at least one of: a number of remotely exploitable vulnerabilities of the entity; a number of security incidents; or a number of vulnerable versions of software of the entity.

Claim	Limitation
5	The method of claim 1, wherein each respective transformation function is a normalization of the respective feature, and further comprising: when the normalization is applied to two or more of the internal security features or the external security features, summing the normalized features.
6	The method of claim 1, wherein determining the internal security rating further comprises weighting the first plurality of transformed features.
7	The method of claim 1, wherein combining the first plurality of transformed features comprises: summing the first plurality of transformed features; and normalizing the summed features by a set of normalization factors.
8	The method of claim 1, wherein combining the second plurality of transformed features comprises: summing the second plurality of transformed features; and normalizing the summed features by a set of normalization factors.
9[pre]	A system for determining a security rating of an entity, the system comprising:

Claim	Limitation
9[a]	one or more computer systems programmed to perform operations comprising:
9[b]	determining an internal security rating comprising:
9[c]	obtaining data indicative of internal security from a plurality of internal data sources;
9[d]	extracting a plurality of internal security features from the obtained data;
9[e]	applying a transformation function to each of the plurality of internal security features; and
9[f]	combining the transformed features to form the internal security rating;
9[g]	determining an external security rating comprising:
9[h]	obtaining data indicative of external security from a plurality of external data sources;
9[i]	extracting a plurality of external security features from the obtained data;
9[j]	applying a transformation function to each of the plurality of external security features; and
9[k]	combining the transformed features to form the external security rating; and
9[l]	providing, via a reporting facility, a composite security rating for the entity based on the internal security rating and the external security rating, wherein at least one of the internal security features or the external security features indicates malicious activity associated with an IP address of the entity.

Claim	Limitation
10	The system of claim 9, wherein the one or more computer systems are further programmed to perform operations comprising: determining the composite security rating based on a weighted combination of the internal security rating and the external security rating.
11	The system of claim 9, wherein the plurality of internal data sources comprises: vulnerability scan data of the entity; data indicating firewall rules of the entity; data from security incident reports corresponding to the entity; data indicative of computer network configurations of the entity; data indicative of software inventory of the entity; data indicative of security policies of the entity; data indicative of security controls of the entity; and data indicative of user behavior corresponding to the entity.
12	The system of claim 9, wherein the internal security features and the external security features comprise at least one of: a number of remotely exploitable vulnerabilities of the entity; a number of security incidents; or a number of vulnerable versions of software of the entity.
13	The system of claim 9, wherein each respective transformation function is a normalization of the respective feature, and wherein

Claim	Limitation
	the one or more computer systems are further programmed to perform operations comprising: when the normalization is applied to two or more of the internal security features or the external security features, summing the normalized features.
14	The system of claim 9, wherein determining the internal security rating further comprises weighting the first plurality of transformed features.
15	The system of claim 1, wherein combining the first plurality of transformed features further comprises: summing the first plurality of transformed features; and normalizing the summed features by a set of normalization factors.
16	The system of claim 9, wherein combining the second plurality of transformed features further comprises: summing the second plurality of transformed features; and normalizing the summed features by a set of normalization factors.

I. INTRODUCTION

The '976 patent relates to a conventional method of gathering internal and external information about an entity's network, generating internal and external scores based on that information, and generating a composite score that combines the internal and external score. But by 2010, the earliest priority date of the '976 patent, assessing a network's security by providing a score that is a composite of internal and external factors was common-place and well-known. As the '976 patent recognizes, "cyber security assessment[s]" were well-known in the art by the time of the patent. EX1001, 1:29-40. Indeed, this petition relies on prior art developed by well-known leaders in the cybersecurity industry, such as a patent application from Cybertrust, a cybersecurity company initially formed by GTE ("Tippett"), combined with a patent filed by the security company McAfee ("McGovern").

Tippett discloses generating a "security risk index" by collecting both internal and external information about an entity's network, generating internal and external "factors" from that information, and then combining the two to create a composite score. When combined with McGovern, the combination also renders obvious well-known and conventional internal sources of information, such as information from vulnerability scans or about network configuration.

II. STANDING

Petitioners certify the '976 patent is available for IPR and they are not estopped.

III. GROUNDS

Petitioners present the below grounds.

Ground	Basis	Reference(s)	Claims
1	§103	Tippett	1-2, 4-10, 12-16
2	§103	Tippett, McGovern	3, 11

IV. POSITA

A person of ordinary skill in the art at the time of the alleged invention (“POSITA”) would have a Bachelor’s degree in Computer Science or similar field and at least two years of industry experience in network security. EX1003, ¶¶48-49. Petitioner further proposes that more education could compensate for less experience and vice versa. *Id.* Petitioner’s expert, Dr. Almeroth, surpassed this level of skill by the earliest filing date of the '976 patent. *Id.*

V. BACKGROUND

A. Technical Background (EX1003, ¶¶50-67)

The '976 patent is directed to collecting information about network resources, generally from external information sources. Prior to 2010, ordinary artisans in the field were aware of numerous techniques for collecting information about a network and its resources using what are known as Open Source Intelligence (“OSINT”)

tools, “open source” indicating that such information could be collected without access to or permission from the target organization.

For example, there were a number of well-known OSINT tools for collecting IP address information about assets. The McNab reference devotes an entire chapter to such methods for “Internet Host and Network Enumeration,” *i.e.* enumerating the various hosts within a network, including their IP addresses.

For example, McNab describes a tool called “whois,” which can look up various information about a domain name, including its authoritative name servers. EX1005, 22.

Example 3-1. Obtaining the domain WHOIS record for blah.com

```
$ whois blah.com
```

```
Domain Name: BLAH.COM
Registrar: NETWORK SOLUTIONS, LLC.
Whois Server: whois.networksolutions.com
Referral URL: http://www.networksolutions.com
Name Server: NS1.BLAH.COM
Name Server: NS2.BLAH.COM
Name Server: NS3.BLAH.COM
Status: clientTransferProhibited
Updated Date: 04-oct-2006
Creation Date: 20-mar-1995
Expiration Date: 21-mar-2009
```

McNab also describes a well-known, free tool called “dig” which can perform a number of functions related to DNS queries. McNab describes using the “dig” command to retrieve a list of hostnames for a specified domain name (“ucia.gov” in

the example below) from a specified name server (“relay2.ucia.gov” in the example below), using a technique called a “DNS zone transfer.” EX1005, 33.

Example 3-8. Using dig to perform a DNS zone transfer

\$ dig @relay2.ucia.gov ucia.gov axfr

```
; <<>> DiG 9.2.4 <<>> ucia.gov @relay2.ucia.gov axfr
;; global options: printcmd
ucia.gov.          3600    IN      SOA     relay1.ucia.gov. root.ucia.gov.
511210023 7200 900 604800 900
ucia.gov.          3600    IN      NS      relay1.ucia.gov.
ucia.gov.          3600    IN      NS      relay7.ucia.gov.
ucia.gov.          3600    IN      NS      auth100.ns.uu.net.
ucia.gov.          3600    IN      MX      5 mail2.ucia.gov.
ain.ucia.gov.      3600    IN      A       198.81.128.68
ain-relay.ucia.gov. 3600    IN      CNAME   relay1.ucia.gov.
ain-relay-int.ucia.gov. 3600    IN      CNAME   ain-relay1-int.ucia.gov.
ain-relay1.ucia.gov. 3600    IN      CNAME   relay1.ucia.gov.
ain-relay1-ext.ucia.gov. 3600    IN      CNAME   relay1.ucia.gov.
ain-relay1-int.ucia.gov. 3600    IN      A       192.168.64.2
ain-relay2.ucia.gov. 3600    IN      CNAME   relay2.ucia.gov.
ain-relay2-ext.ucia.gov. 3600    IN      CNAME   relay2.ucia.gov.
ain-relay2-int.ucia.gov. 3600    IN      A       192.168.64.3
ain-relay7.ucia.gov. 3600    IN      CNAME   relay7.ucia.gov.
ain-relay7-ext.ucia.gov. 3600    IN      CNAME   relay7.ucia.gov.
ain-relay7-int.ucia.gov. 3600    IN      A       192.168.64.67
ex-rtr.ucia.gov.   3600    IN      CNAME   ex-rtr-129.ucia.gov.
ex-rtr-129.ucia.gov. 3600    IN      A       198.81.129.222
ex-rtr-129.ucia.gov. 3600    IN      HINFO   "Cisco 4000 Router" "NP-1E Board"
ex-rtr-191-a.ucia.gov. 3600    IN      A       192.103.66.58
ex-rtr-191-b.ucia.gov. 3600    IN      A       192.103.66.62
foia.ucia.gov.     3600    IN      NS      relay1.ucia.gov.
foia.ucia.gov.     3600    IN      NS      auth100.ns.uu.net.
mail1.ucia.gov.    3600    IN      A       198.81.129.68
mail1out.ucia.gov. 3600    IN      A       198.81.129.71
mail2.ucia.gov.    3600    IN      A       198.81.129.148
mail2out.ucia.gov. 3600    IN      A       198.81.129.146
relay.ucia.gov.    3600    IN      CNAME   relay1.ucia.gov.
relay-int.ucia.gov. 3600    IN      CNAME   ain-relay1-int.ucia.gov.
relay1.ucia.gov.   3600    IN      A       198.81.129.193
relay1-ext.ucia.gov. 3600    IN      CNAME   relay1.ucia.gov.
relay1-int.ucia.gov. 3600    IN      CNAME   ain-relay1-int.ucia.gov.
relay2.ucia.gov.   3600    IN      A       198.81.129.194
relay2-ext.ucia.gov. 3600    IN      CNAME   relay2.ucia.gov.
relay2-int.ucia.gov. 3600    IN      CNAME   ain-relay2-int.ucia.gov.
relay2a.ucia.gov.  3600    IN      A       198.81.129.200
relay2y.ucia.gov.  3600    IN      A       198.81.129.68
relay2z.ucia.gov.  3600    IN      A       198.81.129.69
relay7.ucia.gov.   3600    IN      A       198.81.129.186
relay7-ext.ucia.gov. 3600    IN      CNAME   relay7.ucia.gov.
relay7a.ucia.gov.  3600    IN      A       198.81.129.197
relay7b.ucia.gov.  3600    IN      A       198.81.129.198
res.ucia.gov.      3600    IN      A       198.81.129.116
wais.ucia.gov.     3600    IN      CNAME   relay2.ucia.gov.
```

Once the network hosts have been enumerated, they can then be scanned to assess information about the network. McNab itself explains that “[n]etwork scanners are used to perform bulk automated scanning of IP ranges to identify vulnerable network service components. The two most popular open source network scanners are Nmap and Nessus.” EX1005, 13. Nessus, for example, “is a vulnerability assessment package that can perform many automated tests against a target network, including ICMP, TCP, and UDP scanning, testing of specific network services (such as Apache, MySQL, Oracle, Microsoft IIS, and many others), and rich reporting of vulnerabilities identified.” *Id.* By identifying vulnerabilities, the network can be given a risk assessment score. *Id.*, 390-91.

This process of enumerating network assets and performing vulnerability scans to generate risk assessment scores was described by other sources as well. For example, a 2001 paper titled “An Introduction to Internet Attack & Penetration” (EX1015) describes an “Anatomy of a Hack” that lists the following steps:

1. Identification of Internet-based points of presence
2. Network scanning & reconnaissance
3. Accessing the target system or network
4. Carrying out objectives
5. Manipulation of logs and system files

The paper then goes on to describe attacks such as the exploitation of vulnerabilities, or various forms of malware. EX1015 at 9-14.

In 2002, the National Institute of Standards and Technology (“NIST”) (an organization part of the U.S. Department of Commerce) published a paper called “Risk Management Guide for Information Technology Systems” (EX1016), which provides guidelines and methodologies for conducting risk assessments, mitigating risks, and ensuring the security of IT systems within the federal government. Section 3.1.2 of the paper outlines various information-gathering techniques, such as “Automated Scanning Tool[s]” such as “network mapping tool [to] identify the services that run on a large group of hosts and provide a quick way of building individual profiles of the target IT system(s).” EX1016 at 11-12. This results in a “picture of the IT system environment, and delineation of system boundary.” *Id.* The paper then goes on in Chapter 3.3 to discuss scanning these services to identify vulnerabilities, noting that “[t]he analysis of the threat to an IT system must include an analysis of the vulnerabilities associated with the system environment.” *Id.*, 15. Based on this analysis, the paper recommends producing a risk rating, which is derived “by multiplying the ratings assigned for threat likelihood (e.g., probability) and threat impact,” resulting in various “risk levels of High, Medium, and Low” within a risk-level matrix. *Id.*, 24.

Table 3-6. Risk-Level Matrix

Threat Likelihood	Impact		
			High (100)
High (1.0)	Low 10 X 1.0 = 10	Medium 50 X 1.0 = 50	High 100 X 1.0 = 100
Medium (0.5)	Low 10 X 0.5 = 5	Medium 50 X 0.5 = 25	Medium 100 X 0.5 = 50
Low (0.1)	Low 10 X 0.1 = 1	Low 50 X 0.1 = 5	Low 100 X 0.1 = 10

*Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)*⁸

A 2007 presentation given at the Blackhat conference provides an overview of “gathering and discovery techniques, with a concentration on third-party services and new tools” and then using such tools to “gain[] access to a target network.” EX1017, 4. Thus, in Chapter 3, the paper states “[t]he first step to any security engagement is the initial discovery process,” and describes “discovery techniques, starting from the outside.” *Id.*, 7. The chapter goes on to provide resources for discovering employees of an organization, such as through Google searches, or using a tool called Evolution that “is able to cross-reference information from a large set of public data sources.” *Id.*, 8. The chapter then explains how to use tools to perform “network discovery” using “DNS zone transfers, Whois requests, and reverse DNS lookups.” *Id.*, 9. The chapter then provides descriptions of more advanced tools such as a “‘Domain Dossier’ service which combines the various DNS and Whois requests into [a] single report, with the option to perform a quick port scan as well.”

Id. There is also the “DomainTools.com web site” which “accepts an IP address or host name as an input and provides a list of all domains that reverse back to that IP.”

Id.

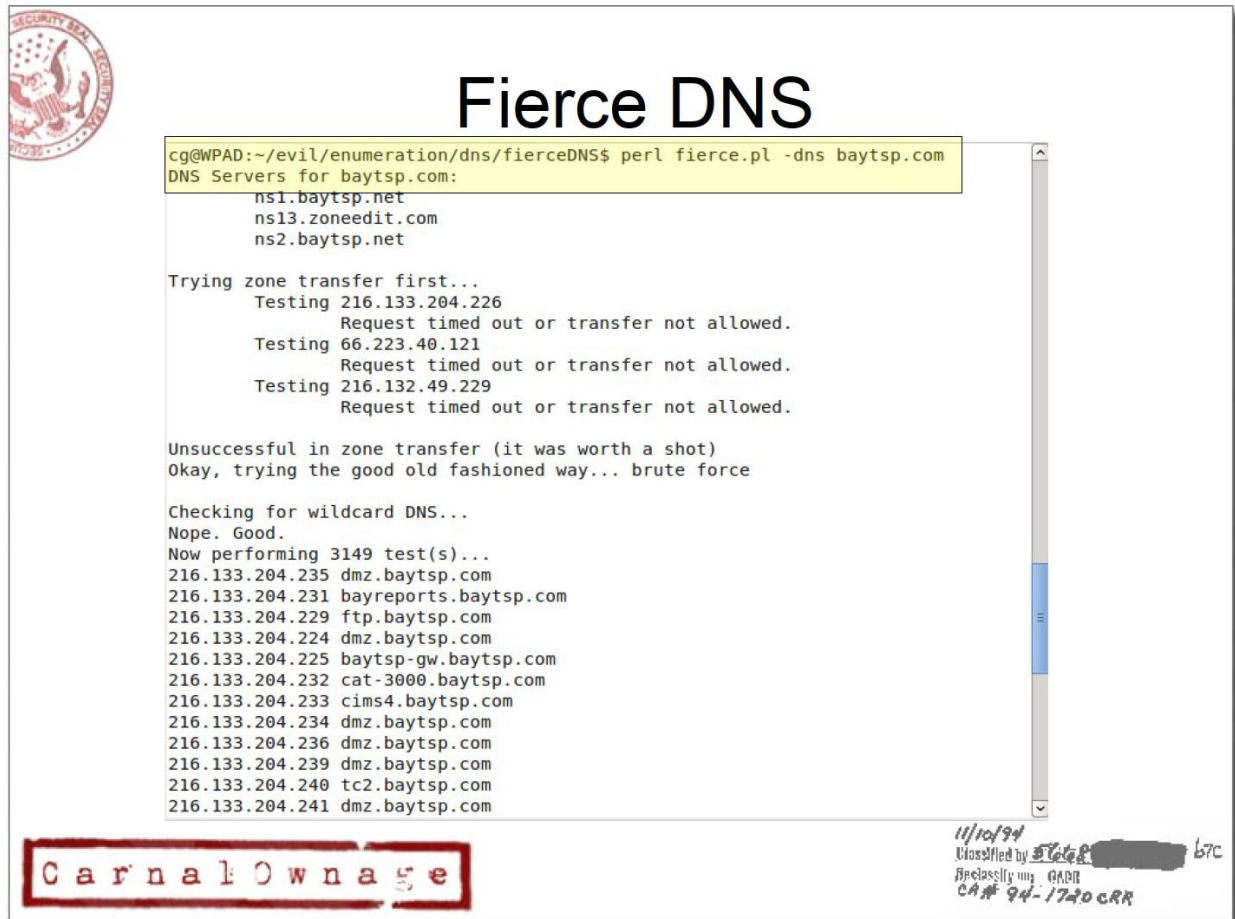
The paper also describes using “the Metasploit Framework” which “includes a number of application discovery modules ... to detect services that are difficult to find otherwise.” *Id.*, 14. For example, the below output searched on an IP range and returned DNS and SNMP services running on hosts within that IP range:

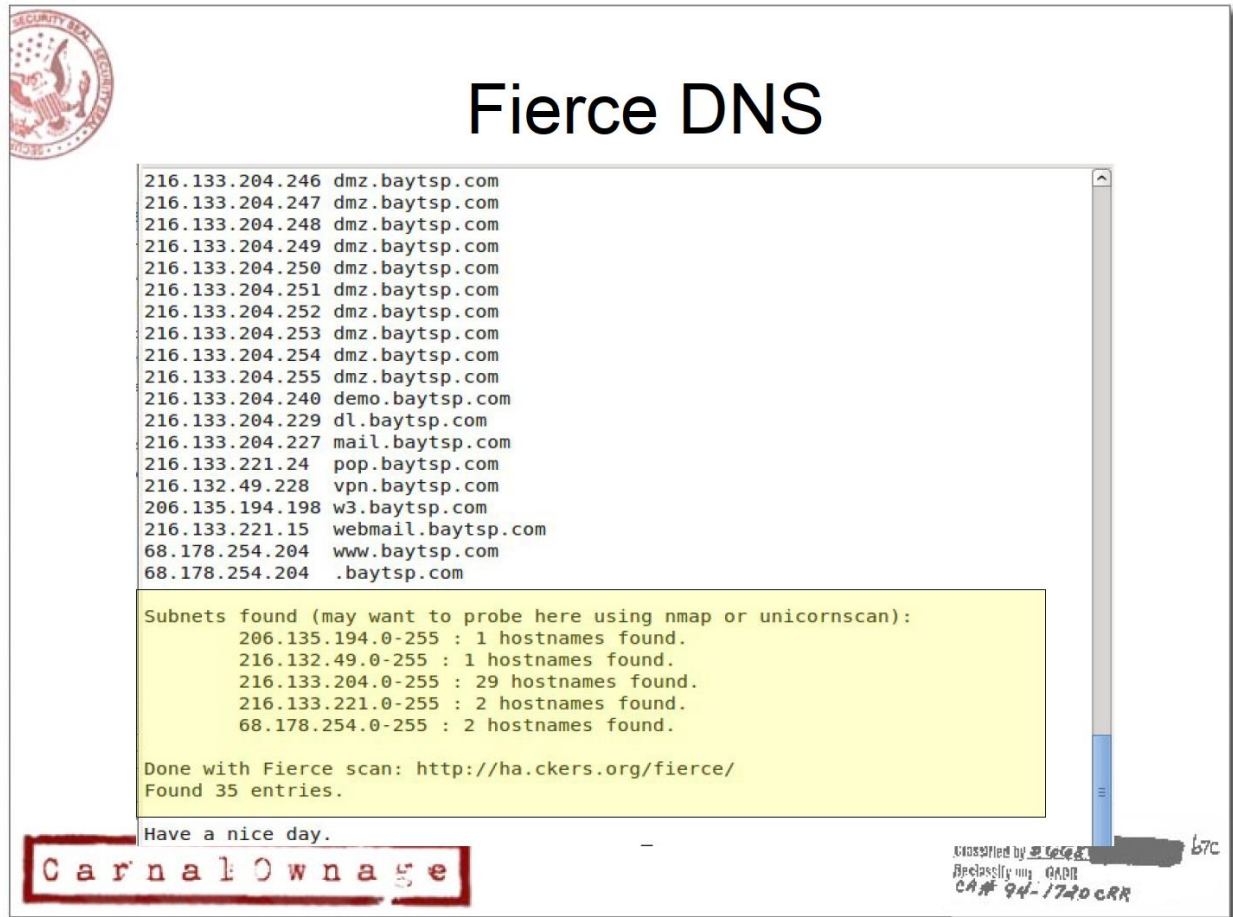
```
[*] Sending 6 probes to xxx.xxx.xxx.0->xxx.xxx.xxx.255 (256 hosts)
[*] Discovered DNS on xxx.xxx.xxx.19 (TinyDNS)
[*] Discovered DNS on xxx.xxx.xxx.249 (BIND 8.4.6-REL-NOESW)
[*] Discovered DNS on xxx.xxx.xxx.250 (Microsoft)
[*] Discovered SNMP on xxx.xxx.xxx.170 (Ethernet Routing Switch)
[*] Discovered SNMP on xxx.xxx.xxx.171 (ProCurve J8692A)
```

Id. The paper goes on to describe various ways to attack these services. *Id.*, 19-33.

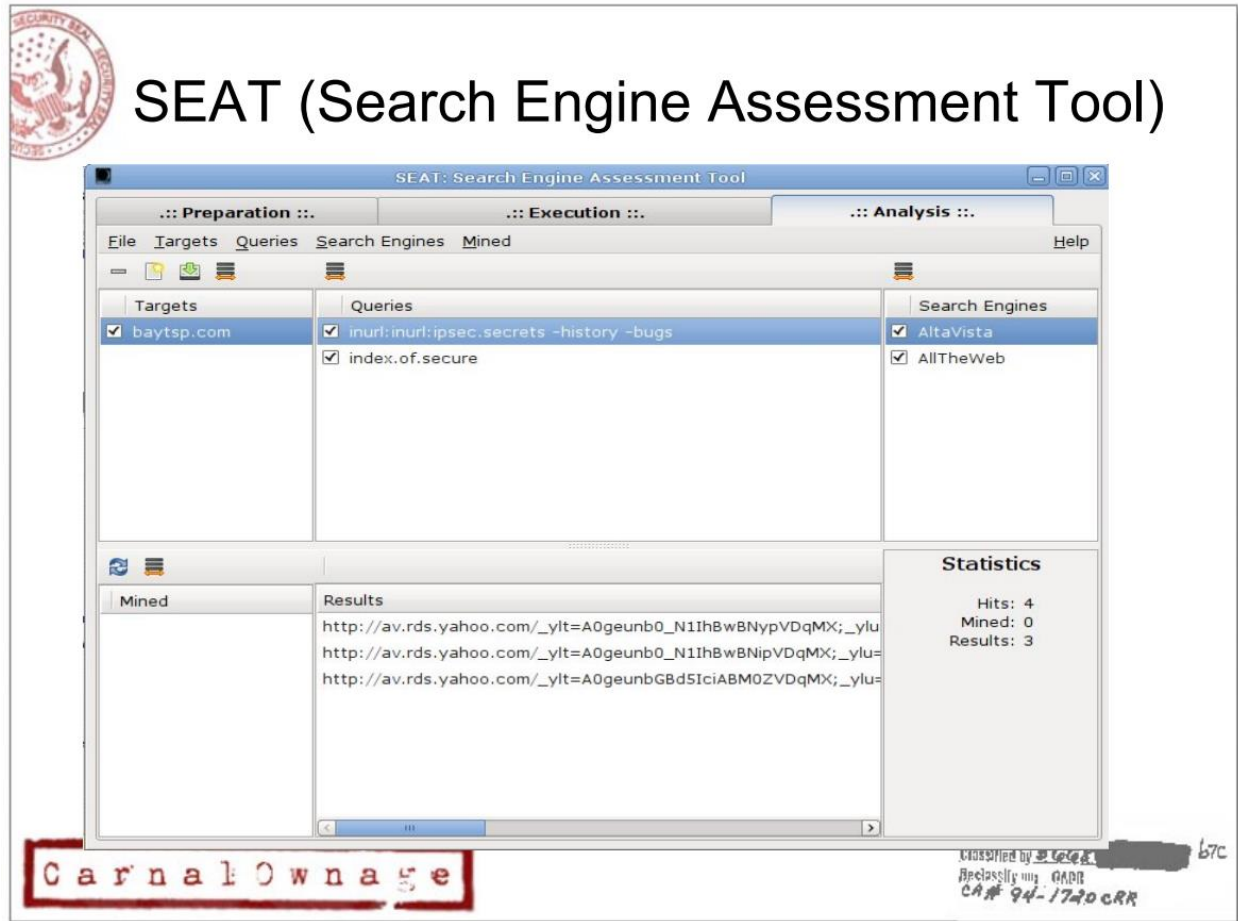
In 2008, a well-known security researcher named Chris Gates delivered a presentation called “New School Information Gathering” (EX1018). The presentation describes a “[b]lack box approach to info gathering” where “the customer wants you to find everything about them you can via ‘open source’ methods.” EX1018 at 5. OSINT information gathering involves “no direct contact with victim’s servers OR no non-standard traffic directed toward victim.” *Id.*, 9. The presentation then describes several tools for gathering such information. For example, the presentation describes one tool called Fierce DNS which “locate[s]

likely targets both inside and outside a corporate network.” *Id.*, 18. Fierce DNS uses a number of DNS queries to find hosts on the same domain and IP blocks used by the domain. *Id.*, 20. The below output for “bytsp.com” shows the various hosts for that domain name. *Id.*, 21-22.





Another tool called “SEAT (Search Engine Assessment Tool)” “uses information stored in search engine databases, cache repositories, and other public resources to scan a site *for potential vulnerabilities*.” *Id.*, 24 (emphasis added). The tool involves providing a domain name as input (such as “baytsp.com” as used in the slides) and returning a set of results about that domain. *Id.*, 26.

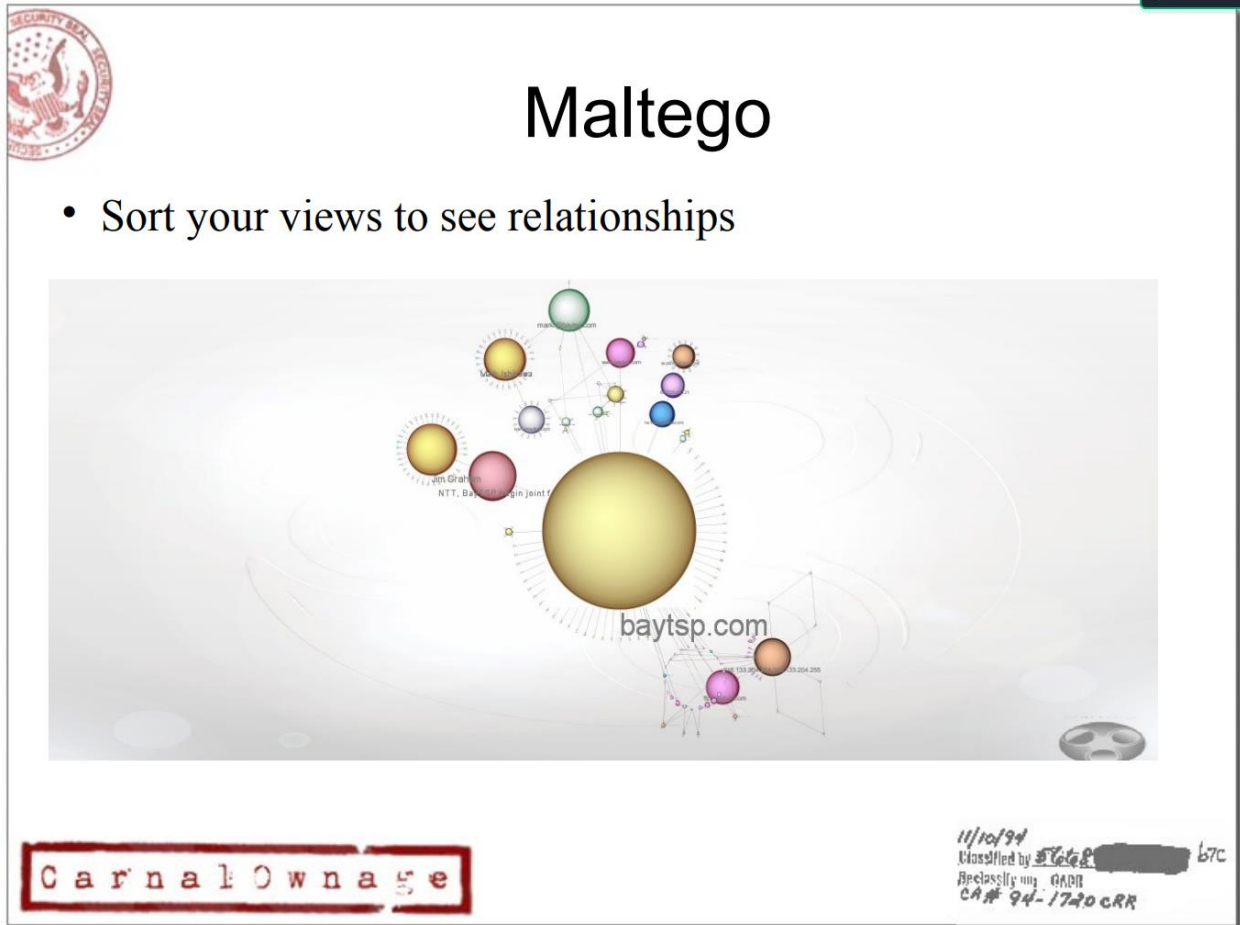


The presentation also describes methods for harvesting email addresses from the provided domain name. *Id.*, 28-32.

Another tool called Metagoofil searches for PDF, Word, and other documents found on the provided domain name and extracts metadata from those documents to, for example, “[r]eveal the creator of a document,” “[r]eveal the application that created the document,” “[r]eveal create date,” all in order to “deliver a directed client side attack for something installed in the enterprise.” *Id.*, 35-40.

Finally, the presentation describes a tool called Maltego, which can perform many of the above functions automatically in one piece of software. Maltego “is a

program that can be used to determine the relationships and real world links between: People ... Companies ... Web sites ... Internet infrastructure such as: Domains, DNS names, Netblocks, IP addresses” and it does this “using open source intelligent (OSINT).” *Id.*, 67. Maltego can enumerate network assets given a domain name, such as by finding “MX and NS servers” for the domain name and determining “what hostnames are shared by the DNS servers,” and “brute forc[ing] our domain names and resolve them to IPs.” *Id.*, 67-72. From there, email addresses and documents can be harvested. *Id.*, 73-77. The presentation explains that Maltego can also search blogs, social networks and incoming links. *Id.*, 82. Maltego also provides graphical representations of the mapped network assets, showing them being associated with various entities. *Id.*, 80.



Maltego is further described and shown at Exhibit 1021, which is a 2009 video entitled “Social Engineering Using Maltego.” The video shows how Maltego can be used to discover network assets for a particular domain, as well as additional domains that share a DNS name server.

Thus, as shown above, ordinary artisans had long had experience seeking information from various sources to enumerate network assets and collect information for providing a risk assessment score.

B. Public Availability

McNab and other exhibits discussed in this Petition were publicly available before September 24, 2010, as discussed below. EX1003, ¶¶75-88.

1. McNab

McNab is entitled “Network Security Assessment” and is a book published by O’Reilly Media in 2008. EX1005, 5. According to Dr. Hall-Ellis and her review of library records, McNab was publicly available at the Penrose Library at the University of Denver by November 10, 2008. EX1014, ¶44. She also notes that the Library of Congress created a catalog entry for the book by June 8, 2009. *Id.*, ¶45. Thus, she concludes that McNab was available by 2008, and further concludes that Exhibit 1005 is a true and correct copy as it was published in 2008. *Id.*, ¶¶42, 48.

Dr. Almeroth also agrees that McNab was indexed and made available to those of skill in the art by 2008 based on his personal knowledge and as an expert in the field, because O’Reilly Media is “a reputable publisher such that copyright dates on their publications are a reliable and trustworthy indicator of when the publication was published.” EX1003, ¶¶76-79. Thus, he also concludes that McNab was publicly available by 2008 and that Exhibit 1005 is a true and correct copy as it was published in 2008. *Id.*

2. Internet Archive Pages

Exhibits 1015, 1017, 1020, and 1022 are webpages and documents from the Internet Archive’s Wayback Machine. According to Mr. Frank-White, the Wayback

Machine archives webpages “by use of web archiving software that automatically stores copies of files available via the Internet, each file preserved as it existed at a particular point in time.” EX1013, ¶4. Each Internet Archive URL contains the date and time when the webpage was archived. *Id.*, ¶5. All of the Internet Archive exhibits are dated before September 24, 2010, and thus indicate that they were publicly available on the Internet before that date, that the copies attached at 1015, 1017, 1020, and 1022 are true and correct copies of the webpage on the date they were archived.

Dr. Almeroth, who is familiar with the Wayback Machine, agrees with Mr. Frank-White and agrees that the Internet Archive exhibits are archives of publicly available webpages at the time they were archived as indicated in the exhibits’ URL, and that those exhibits are true and correct copies. EX1003, ¶¶80-81; *see Valve Corp. v. Ironburg Inventions, Ltd.*, 8 F.4th 1364, 1374-75 (Fed. Cir. 2021) (Wayback Machine webpages are “highly persuasive evidence of public accessibility”).

3. Public Videos

Exhibits 1019 and 1021 are printed webpages from Vimeo and YouTube, respectively. Vimeo and YouTube are video-hosting sites, and the URLs for Exhibits 1019 and 1021 link to videos hosted on those sites. Exhibit 1019 is a video of Chris Page presenting the slideshow at Exhibit 1018. Exhibit 1021 is a video

providing a demonstration of the Maltego product. Exhibit 1031 are screenshots of relevant portions of the YouTube video at Exhibit 1021.

Dr. Almeroth opines that Vimeo’s indication that Exhibit 1019’s video was uploaded on January 6, 2009 is “generally a reliable indicator of when a video was publicly available.” EX1003, ¶¶82-85. In addition, Exhibit 1020 provides corroboration that the video was available in 2009, since it is a March 2, 2009 archived link of the Vimeo webpage. Thus, Dr. Almeroth opines that the video linked at Exhibit 1019 was publicly available by early 2009 and is a true and correct copy. *Id.* Moreover, Ms. Melissa Nezhnik of Vimeo’s Trust and Safety group confirmed that the video at Exhibit 1019 was “uploaded on January 6, 2009” by the user “carnal0wnage.” Ex. 1029.

Dr. Almeroth also opines that YouTube’s date of September 14, 2009 for Exhibit 1021 is also generally reliable. EX1003, ¶¶86-88. Because the video has thousands of views, he also opines that it was publicly available by 2009, and that it was indexed by YouTube, like all uploaded videos are by default. *Id.* He also notes that the video itself shows dates from early 2009, providing corroborating evidence of the date of its public availability, and that it is a true and correct copy. *Id.* Metadata about the YouTube video indicates that it was “publishedAt” September 14, 2009 and has a “viewCount” of 60,168 views, thereby further indicating its public availability by 2009. EX1030.

Analogous to the Federal Circuit’s recognition that Wayback Machine webpages are “highly persuasive evidence of public accessibility,” pages from YouTube and Vimeo are likewise persuasive evidence of public accessibility because they are “prominent or well-known among persons of ordinary skill in the art.” *M & K Holdings, Inc. v. Samsung Electronics Co.*, 985 F. 3d 1376, 1381 (Fed. Cir. 2021). In addition, the Board has held that the date provided by the YouTube website along with testimonial support from an expert is enough evidentiary support to establish the video’s public availability. *Mission Integrated Technologies, LLC v. Clemente*, IPR2023-01285, Paper 16 at 22-23 (PTAB Feb. 23, 2024).

C. ’976 patent

The ’976 patent to Boyer *et al.* was filed October 13, 2020, and claims priority to a provisional application filed September 24, 2010.

The ’976 patent is directed to conventional techniques for measuring the security vulnerability of a network from internal and external characterizations. EX1003, ¶¶68-69. Although the Abstract describes the purported invention as “creating a composite security rating” from data that is “derived from externally observable characteristics,” the claims require both internal and external data sources. EX1001, Abstract; cl. 1. In particular, the independent claims recite an internal security and an external security rating, which are then combined to a composite security rating. EX1003, ¶¶68-69.

1. Prosecution History (EX1003, ¶¶70-72)

During prosecution, the applicant's initial set of claims was significantly different than the claims that were eventually allowed. EX1002, 598. Below is the language of the original claim 1:

1. (Original) A method of evaluating information security of a third party computer system, the method comprising:
collecting at least two security characterizations of the third party computer system;
generating a composite security rating using the at least two security characterizations;
wherein the two security characterizations are derived from externally observable characteristics of the third party computer system.

After the examiner issued a non-final rejection over U.S. Pub. No. 2006/0212925 ("Shull"), the applicant canceled the claim and drafted a new set of claims, arguing that Shull did not disclose an internal security rating, an external security rating, or providing a composite security rating. EX1002, 311-314. The examiner then issued a notice of allowance.

VI. CLAIM CONSTRUCTION

The claim terms should be given their plain and ordinary meaning under *Phillips*. EX1003, ¶¶73-74.

VII. GROUNDS

A. Ground 1: Tippet

1. Claim 1

(a) 1[pre]: A method for determining a security rating of an entity, the method comprising:

Tippett discloses a method for determining a “security risk index,” *i.e.* ***security rating***, for an entity. One of the security risk indices disclosed by Tippett is a “local security risk index representing the security of ... information resources associated with [an] entity 224A.” EX1006 at ¶46; EX1003 at ¶¶89-90. Information resources include an entity’s “databases,” “computer terminals,” or “servers.” *Id.* at ¶32. Tippett discloses that an “entity” can “include ... an organization; ... or any other entity,” as well as “consultants, vendors, customers, home users.” *Id.*

(b) 1[a]: determining an internal security rating comprising:

Tippett discloses that determining the “local security risk index,” *i.e.* ***consolidated security rating***, includes determining a “local vulnerability factor,” *i.e.* ***internal security rating***. EX1006 at ¶47; EX1003 at ¶¶91-92. Specifically, Tippett discloses that the local security risk index is expressed as “ $LSRI = GT * LV * GI$ ” where “LV may be associated with a local vulnerability factor.” *Id.* Tippett further discloses that the “local vulnerability factor” includes “***internal*** factor component[s]” such as a “mitigating measure designed to secure [the entity’s] information resources, a past history of at least one type of security breach, a future plan for securing the information resources associated with the entity 224A, or any other type of query related to the local vulnerability of the information resources associated with the entity 224A,” thereby indicating that the “local vulnerability factor” is an ***internal security rating***. EX1006 at ¶¶24, 49. In addition, as discussed

in the next limitation, because the “local vulnerability factor” is generated from information from internal data sources, it is an ***internal security rating***.

(c) **1[b]: obtaining data indicative of internal security from a plurality of internal data sources;**

Tippett discloses that generating the “local vulnerability factor,” *i.e.* ***internal security rating***, comprises gathering “local vulnerability factor components,” which involves obtaining ***data indicative of internal security***. Such local vulnerability factor components are generated from information relating to “a mitigating measure designed to secure [the entity’s] information resources, a past history of at least one type of security breach, a future plan for securing the information resources associated with the entity 224A, or any other type of query related to the local vulnerability of the information resources associated with the entity 224A,” each of which are ***data indicative of internal security*** since they indicate the vulnerability of the entity based on internal past events or internal mitigating measures. EX1006 at ¶49. Because such information is indicative of the internal state of the entity’s network, a POSITA would understand that such information is obtained from ***a plurality of internal data sources***. EX1003 at ¶¶93-94.

Moreover, Tippett describes that such components are “internal factor component[s],” thereby indicating that the data is ***obtained from a plurality of internal data sources***. EX1006 at ¶24; EX1003 at ¶95. Indeed, Tippett discloses that the security risk index “determining unit” receives information from the entity

via “an information link” or “one or more networks,” and that an entity has “various information resources ... such as one or more databases 232, one or more computer terminals 234, one or more computer networks 236, one or more servers 238,” *i.e. a plurality of data sources that are internal to the entity’s network*. EX1006 at ¶¶31-32.

Alternatively, a POSITA would have found it obvious that the local vulnerability factor components are obtained from a plurality of internal data sources. EX1003 at ¶96. In particular, a POSITA would have been motivated to store information such as the entity’s mitigating measures, history of security breaches, or future security plans (EX1006 at ¶49) within *internal* data sources because such information would be unique to the entity as well as sensitive and confidential to the entity and therefore undesirable to be stored outside of the entity’s control. EX1003 at ¶96. A POSITA would also be motivated to store such information within a *plurality* of data sources because multiple data sources provide redundancy and parallelization, thereby increasing efficiency. *Id.* Moreover, Tippettt already discloses that the entity’s information resources include multiple “databases,” *i.e. internal data stores*, and that the entity sends information to the security risk index determining unit, thus further motivating a POSITA to store such information within the already-present internal data stores. EX1006 at ¶¶31-32. A POSITA would have a reasonable expectation of success because storing security

information in databases was conventional and well-within the skill of an ordinary artisan. EX1003 at ¶96.

(d) **1[c]: extracting a plurality of internal security features from the obtained data;**

Tippett discloses that “local vulnerability factor components,” *i.e. plurality of internal security features*, are extracted from the internal security data. EX1003 at ¶¶97-98. In particular, such factor components are “**determined based on** the at least one standard or customized local vulnerability query related to the presence of at least one mitigating measure designed to secure information resources, a past history of at least one type of security breach, a future plan for securing the information resources associated with the entity 224A, or any other type of query related to the local vulnerability of the information resources associated with the entity 224A.” EX1006 at ¶49.

(e) **1[d]: applying a respective transformation function to each of the plurality of internal security features to determine a first plurality of transformed features; and**

Tippett discloses that the local vulnerability factor components, *i.e. internal security features*, are weighted, *i.e. applied a respective transformation function*. EX1003 at ¶¶99-100. In particular, Tippett discloses that the “local vulnerability factor component weighting operation” yields a “weighted local vulnerability factor component,” *i.e. a first plurality of transformed features*. EX1006 at ¶51. Tippett

describes that the weighting process includes “evaluating the effectiveness of the specific implemented mitigating measure according to one or more different aspects of mitigation.” EX1006 at ¶52. Tippet also describes a weighting process wherein “more than one implemented mitigating measure may safeguard against a same specific type of security event,” which uses the formula:

$$LVFC=1-((1-E_1)\cdot(1-E_2)\cdot\ldots(1-E_n)),$$

This weighting process would be used for a “local vulnerability factor component for the specific type of security event.” *Id.* at ¶53. In other words, Tippet describes at least a weighting process for a local vulnerability factor component representing a mitigating measure and a weighting process for a component representing a security event (such as a breach). EX1003 at ¶101. Thus, Tippet describes *respective transformation functions* depending on the type of component, *i.e. internal security feature*.

(f) 1[e]: combining the first plurality of transformed features to form the internal security rating;

Tippet teaches that the weighted local vulnerability factor components, *i.e. first plurality of transformed features*, are “combined ... using statistical mathematics, Bayesian logic, sampling and mitigating measurement, or another method” to generate the “local vulnerability factor,” *i.e. internal security rating*. EX1006 at ¶54; EX1003 at ¶¶102-03.

(g) **1[f]: determining an external security rating comprising:**

Tippett discloses that determining the “local security risk index,” *i.e.* **consolidated security rating**, includes determining a “general threat factor,” *i.e.* **external security rating**. EX1006 at ¶47; EX1003 at ¶¶104-05. Specifically, Tippett discloses that the local security risk index is expressed as “ $LSRI=GT*LV*GI$ ” where “GT may be associated with a general threat factor.” *Id.* Tippett further discloses that the “general threat factor” includes information about “new types of security events and their severity, information relating to future security events discovered in chat rooms or on message boards, current trends in the implementation of security events, or any other data related to security events that have transpired on the network 228.” *Id.* at ¶37. Tippett further clarifies that a “security event may be any event that threatens the security of one or more information resources, such as, an electronic event, a physical event, an intentional event, an unintentional event, a man-made event, a natural event, an internal event, an external event, a system event, a non-system event, or other event.” *Id.*

A POSITA would have understood that the “general threat factor” is an **external security rating**. EX1003 at ¶106. As an initial matter, as discussed in the next limitation, because the information to generate the “general threat factor” is obtained from external data sources, that is enough to be an **external security rating**. In addition, the “general threat factor” is a characteristic of “network 228,” of which

the comprises the networks of multiple entities. EX1006 at ¶¶37, 32, Fig. 2. This is analogous to the '976 patent's disclosure of "industry reports" as an external source for the external security rating, which indicates that the external security rating can be a characteristic of a larger network of which the entity is just one part. Ex. 1001, 14:47-49.

To the extent Patent Owner argues that the *external security rating* must be a characteristic specific to just the entity, this is also disclosed in Tippet. EX1003 at ¶107. Specifically, Tippet discloses that the "general threat factor" is generated from information from "information sources 242." EX1006 at ¶37. Such information sources contain information "pertaining to security events that threaten the security of the *information resources* ... on the network 228," which Tippet discloses are resources of an entity. *Id.* at ¶¶33, 32 ("The entity 224A may be associated with various *information resources* ... such as one or more databases 232, one or more computer terminals 234, one or more computer networks 236, one or more servers 238, and one or more other information resources 240."). In other words, because the external information sources contain information about specific information resources on the network, this would include information about resources belonging to the entity. EX1003 at ¶107.

- (h) **1[g]: obtaining data indicative of external security from a plurality of external data sources;**

Tippett discloses that generating the “general threat factor,” *i.e.* **external security rating**, comprises gathering “general threat factor components,” which involves obtaining **data indicative of external security**. EX1003 at ¶¶108-09. In particular, the general threat factor components are generated from obtained data “pertaining to security events that threaten the security of the information resources and the frequency or rate at which they occur on the network.” EX1006 at ¶37. Such data includes “new types of security events and their severity, information relating to future security events discovered in chat rooms or on message boards, current trends in the implementation of security events, or any other data related to security events that have transpired on the network 228.” *Id.* A POSITA would understand that such data is **indicative of external security** because they include “external event[s]” and are information directed to events that are external to the entity and not specific to the entity, such as information about new vulnerabilities or mitigating measures found on “chat rooms or on message boards.” *Id.*; EX1003 at ¶109. Indeed, the “general threat factor components” are data pertaining to security events on “the network,” which is broader than the particular entity and contains multiple entities. *See id.* at ¶¶31-32.

Tippett further discloses that such information is obtained “from the plurality of information sources 242,” which include **external data sources** such as “public databases, network chat forums, network message boards, scholarly journals,

periodicals, personal and commercial web pages, sensors, machine records, trust values, or any other source of information.” EX1006 at ¶¶37, 33. Because such information is about security events or mitigating measures that are not specific to an organization, and may be of interest to any security researcher, a POSITA would understand that such sources are **external** and not within the control of the entity. EX1003 at ¶110.

(i) **1[h]: extracting a plurality of external security features from the obtained data;**

Tippett discloses that “global threat factor components,” *i.e.* **plurality of external security features**, are extracted from the external security data. In particular, such factor components are generated by “**obtaining data** ... pertaining to security events that threaten the security of the information resources and the frequency or rate at which they occur on the network 228.” EX1006 at ¶37; EX1003 at ¶¶111-12.

(j) **1[i]: applying a respective transformation function to each of the plurality of external security features to determine a second plurality of transformed features; and**

Tippett discloses that the global threat factor components, *i.e.* **external security features**, are normalized and weighted, *i.e.* **applied a respective transformation function**. In particular, Tippett discloses that a “general threat factor component ... may be in the form of a rate, a frequency, a count, a scale, or another

form” and therefore must be “convert[ed] ... into a common format” by a “normalizing operation.” EX1006 at ¶38. A POSITA would understand that the normalization operation, *i.e. transformation function*, is specific to the form of the component, and therefore is a *respective transformation function*. EX1003 at ¶¶113-14.

Tippett also discloses that the global threat factor components are “weighted,” such as “based on ... the severity of a possible security event, the probability of a future security event, the predictability of a possible security event, or any other basis.” EX1006 at ¶¶38-39. Thus, the weighting formula is also a *respective transformation function*. EX1003 at ¶115.

Once these transformation functions are applied, this results in a “normalized and weighted” “general threat factor component,” *i.e. a second plurality of transformed features*. EX1003 at ¶116.

(k) 1[j]: combining the second plurality of transformed features to form the external security rating; and

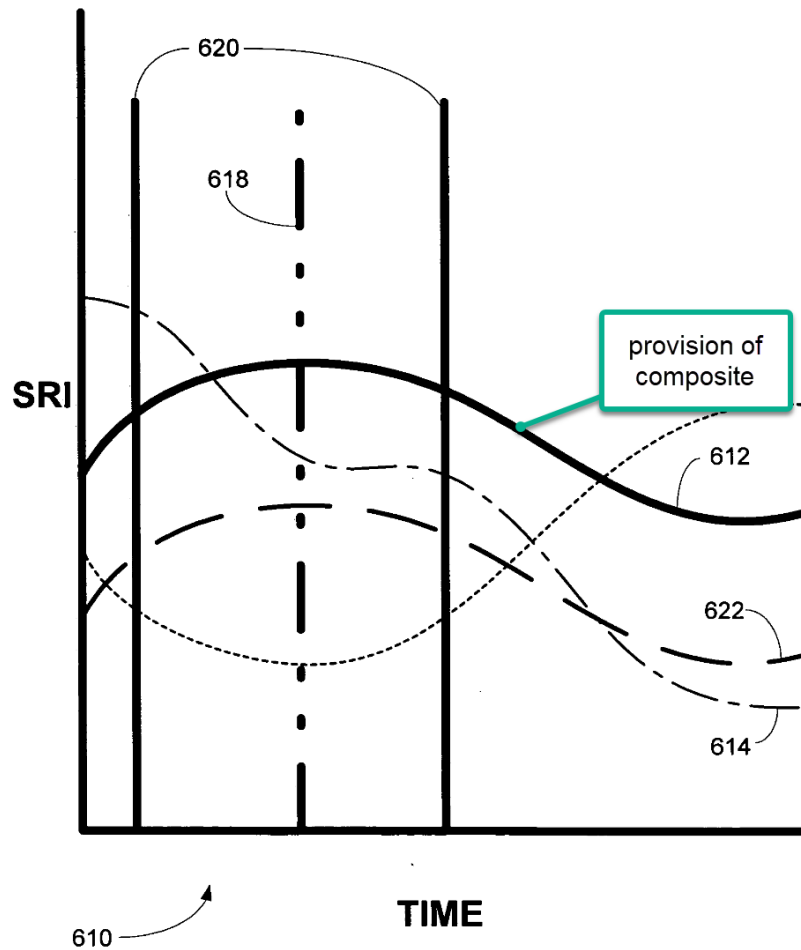
Tippett teaches that the normalized and weighted general threat factor components, *i.e. second plurality of transformed features*, are “combined ... using statistical mathematics, Bayesian logic, sampling and measurement, or another method” to generate the “general threat factor,” *i.e. external security rating*. EX1006 at ¶39; EX1003 at ¶¶117-18.

- (l) **1[k]: providing, via a reporting facility, a composite security rating for the entity based on the internal security rating and the external security rating, wherein at least one of the internal security features or the external security features indicates malicious activity associated with an IP address of the entity.**

“a composite security rating for the entity based on the internal security rating and the external security rating”: Tippet discloses that it combines the “local vulnerability factor” (i.e. ***internal security rating***) and the “general threat factor” (i.e. ***external security rating***) to generate a “local risk index representing the security of ... information resources associated with [an] entity 224A,” i.e. ***a composite security rating for the entity***. EX1006 at ¶46; EX1003 at ¶¶119-20. In particular, the “local risk index” can be calculated using the formula “LSRI=GT*LV*GI” where “LV may be associated with a local vulnerability factor” and “GT may be associated with a general threat factor.” *Id.* at ¶47.

“providing, via a reporting facility, a composite security rating”: Tippet discloses a “graphical representation,” i.e. ***a reporting facility***, to provide a “local security risk index” for a particular entity. EX1006 at ¶57; EX1003 at ¶121. Figure 6 is an example of the graphical representing, where elements 612 and 614 are different local security risk indices for different entities. *Id.*

FIG. 6



“wherein at least one of the internal security features or the external security features indicates malicious activity associated with an IP address of the entity”: Tippet discloses that the “local vulnerability factor” (i.e. *internal security feature*) is generated from information about “a past history of at least one type of *security breach*” that occurred on the entity’s network. EX1006 at ¶¶49, 48 (“This may include adding or subtracting at least one local vulnerability query such as, a type of possible security breach that is *unique ... to the entity 224A.*”); EX1003 at

¶122. A POSITA would understand that a security breach of a network is ***malicious activity associated with an IP address of the entity***, because a security breach is almost always a breach of a network node which contains an IP address that belongs to the entity's network. EX1003 at ¶122. For example, information about a breach of a computer belonging to an entity's employee would be ***malicious activity associated with an IP address*** of that employee's computer, which is an ***IP address of the entity***. *Id.*

2. **Claim 2: The method of claim 1, further comprising: determining the composite security rating based on a weighted combination of the internal security rating and the external security rating.**

As discussed above for limitation 1[k], the “local security risk index” (*i.e.* ***composite security rating***) is generated by ***combining*** the “general threat factor” (*i.e.* ***external security rating***) and “local vulnerability factor” (*i.e.* ***internal security rating***). EX1006 at ¶47. The combination is a ***weighted combination***, because as discussed in limitations 1[d] and 1[i], the “general threat factor” and “local vulnerability factor” are made up of weighted components. EX1003 at ¶¶123-24. As a result, each factor as a whole is also weighted in accordance with the weight of its components. *Id.*

3. **Claim 4: The method of claim 1, wherein at least one of the internal security features or the external security features comprise at least one of: a number of remotely exploitable vulnerabilities of the entity; a number of security incidents; or a number of vulnerable versions of software of the entity.**

Tippett discloses that at least one of the components of the “local vulnerability factor” (*i.e.* ***internal security feature***) is derived from data regarding the “past history of at least one type of security breach.” EX1006 at ¶49. A POSITA would understand that a history of security breaches of the entity would include ***a number of security incidents***, specifically the number of times that type or types of security breach occurred in the recorded history. EX1003 at ¶¶125-26.

4. **Claim 5: The method of claim 1, wherein each respective transformation function is a normalization of the respective feature, and further comprising: when the normalization is applied to two or more of the internal security features or the external security features, summing the normalized features.**

As discussed for limitation 1[i], Tippett discloses performing a ***respective transformation function*** on ***external security features*** in the form of a “normalizing operation.” EX1006 at ¶38; EX1003 at ¶¶127-28.

To the extent Patent Owner argues that the claim requires that the ***internal security features*** also be normalized, a POSITA would have found it obvious to normalize the “local vulnerability factor components,” *i.e.* ***internal security features***. EX1003 at ¶129. A POSITA would be motivated to normalize the local vulnerability factor components because, as taught by Tippett itself, normalizing provides the benefit of “convert[ing]” a component “into a common format,” which is needed if the component “may be in the form of a rate, a frequency, a count, a scale, or another form.” EX1006 at ¶38; EX1003 at ¶129. A POSITA would have

understood that the “local vulnerability factor components” may also come in different forms, especially since they are described as having different forms, *i.e.* “a mitigating measure,” “a past history ... of security breach,” or “a future plan.” EX1006 at ¶49; EX1003 at ¶129. Thus a POSITA would be motivated to normalize these components into a common format so that they can be combined into the local vulnerability factor. EX1003 at ¶129. A POSITA would have had a reasonable expectation of success in doing so because normalization is itself taught by Tippet and would have been well within the skill of a POSITA, such as by converting the factor component into a common scale. *Id.* For example, both a mitigating measure and future plan can be normalized to a scale of 1-10 depending on their known efficacy against vulnerabilities. *Id.*

Tippet further discloses that the normalized factor components are “combined ... using statistical mathematics, Bayesian logic, sampling and measurement, or another method.” EX1006 at ¶¶39, 54. A POSITA would understand that such methods of combination would include **summing** the components (*i.e. the normalized features*), since summing is the simplest and most straightforward method of using “mathematics” to combine the components. EX1003 at ¶130.

5. **Claim 6: The method of claim 1, wherein determining the internal security rating further comprises weighting the first plurality of transformed features.**

As discussed for limitation 1[d], Tippet discloses that the local vulnerability factor components are weighted. *See* EX1006 at ¶¶51-52. Furthermore, as discussed for claim 5, a POSITA would have found it obvious to normalize the local vulnerability factor components as the transformation function that results in a ***first plurality of transformed features***. EX1003 at ¶¶131-32. Thus, for the same reasons, a POSITA would have also found it obvious to perform the weighting as taught by Tippet after the normalization, especially since Tippet expressly teaches that other factor components are “normalized and weighted.” *See, e.g.*, EX1006 at ¶39; EX1003 at ¶132.

6. Claim 7: The method of claim 1, wherein combining the first plurality of transformed features comprises: summing the first plurality of transformed features; and normalizing the summed features by a set of normalization factors.

As discussed in limitations 1[d] and 1[e], Tippet discloses that the local vulnerability factor components are weighted to result in a ***first plurality of transformed features***. Tippet further discloses that the weighted components are “combined ... using statistical mathematics, Bayesian logic, sampling and mitigating measurement, or another method” to generate the “local vulnerability factor.” EX1006 at ¶54. A POSITA would understand that such methods of combination would include ***summing*** the components, since summing is the simplest and most straightforward method of using “mathematics” to combine the components. EX1003 at ¶¶133-34.

Tippett further discloses that the “local vulnerability factor,” *i.e.* **summed features**, are normalized by multiplying it with the “general impact factor,” *i.e.* **set of normalization factors**. EX1006 at ¶47. The “general impact factor” is the combination of various components that “reflect all ... effects associated with a security breach” such as “the hard and soft costs of a security breach such as the cost of previous security breaches, the future cost of predicted security breaches, public sentiment with regard to security breaches, or other information” and represents “an expected cost of a breach of the security of the information resources.” EX1006 at ¶¶43, 23. Thus, in conjunction with the “local vulnerability factor,” which “represent[s] ... a likelihood of a security event breaching the security of the information resources” (EX1006 at ¶23), the “general impact factor” acts as a **set of normalization factors** for each of the “local vulnerability factor components” that make up the “local vulnerability factor.” EX1003 at ¶135. This is because each “general impact factor component” describes the effect of a security event and each “local vulnerability factor component” describes the likelihood of the security event, and thus when they are multiplied together, it normalizes the “local vulnerability factor components” into a value that represents the security event’s expected harm (*i.e.* probability of harm multiplied by the magnitude of harm) particular to an entity. *Id.*

7. **Claim 8: The method of claim 1, wherein combining the second plurality of transformed features comprises:**

summing the second plurality of transformed features; and normalizing the summed features by a set of normalization factors.

As discussed in limitations 1[i] and 1[j], Tippet discloses that the general threat factor components are weighted to result in ***a second plurality of transformed features***. Tippet further discloses that the weighted components are “using statistical mathematics, Bayesian logic, sampling and measurement, or another method” to generate the “general threat factor.” EX1006 at ¶39. A POSITA would understand that such methods of combination would include ***summing*** the components, since summing is the simplest and most straightforward method of using “mathematics” to combine the components. EX1003 at ¶¶136-37.

Tippet further discloses that the “general threat factor,” *i.e.* ***summed features***, are normalized by multiplying it with the “general impact factor,” *i.e.* ***set of normalization factors***. EX1006 at ¶47. The “general impact factor” is the combination of various components that “reflect all ... effects associated with a security breach” such as “the hard and soft costs of a security breach such as the cost of previous security breaches, the future cost of predicted security breaches, public sentiment with regard to security breaches, or other information” and represents “an expected cost of a breach of the security of the information resources.” EX1006 at ¶¶43, 23. Thus, in conjunction with the “general threat factor,” which “represent[s] ... a rate or frequency of security events that threaten the security of the information

resources” (EX1006 at ¶23), the “general impact factor” acts as a ***set of normalization factors*** for each of the “general threat factor components” that make up the “general threat factor.” EX1003 at ¶138. This is because each “general impact factor component” describes the effect of a security event on a network and each “general threat factor component” describes the rate of the security event threatening a network and thus when they are multiplied together, it normalizes the “general threat factor components” into a value that represents the security event’s expected harm (*i.e.* probability of harm multiplied by the magnitude of harm) to a network. *Id.*

8. Claim 9

(a) 9[pre]: A system for determining a security rating of an entity, the system comprising:

See limitation 1[pre]. Tippet discloses a “system.” EX1006 at Abstract; EX1003 at ¶139.

(b) 9[a]: one or more computer systems programmed to perform operations comprising:

Tippet discloses that its system and methods are performed through “software modules running in a distributed computing environment,” *i.e.* ***computer systems programmed to perform operations***. EX1006 at ¶30; EX1003 at ¶140.

(c) 9[b]: determining an internal security rating comprising:

See limitation 1[a]. EX1003 at ¶141.

- (d) 9[c]: obtaining data indicative of internal security from a plurality of internal data sources;**

See limitation 1[b]. EX1003 at ¶142.

- (e) 9[d]: extracting a plurality of internal security features from the obtained data;**

See limitation 1[c]. EX1003 at ¶143.

- (f) 9[e]: applying a transformation function to each of the plurality of internal security features; and**

See limitation 1[d]. This limitation is broader than limitation 1[d] as it does not require that the transformation function be a “*respective* transformation function.” EX1003 at ¶144.

- (g) 9[f]: combining the transformed features to form the internal security rating;**

See limitation 1[e]. EX1003 at ¶145.

- (h) 9[g]: determining an external security rating comprising:**

See limitation 1[f]. EX1003 at ¶146.

- (i) 9[h]: obtaining data indicative of external security from a plurality of external data sources;**

See limitation 1[g]. EX1003 at ¶147.

- (j) 9[i]: extracting a plurality of external security features from the obtained data;**

See limitation 1[h]. EX1003 at ¶148.

- (k) 9[j]: applying a transformation function to each of the plurality of external security features; and**

See limitation 1[i]. This limitation is broader than limitation 1[i] as it does not require that the transformation function be a “**respective** transformation function.” EX1003 at ¶149.

- (l) **9[k]: combining the transformed features to form the external security rating; and**

See limitation 1[j]. EX1003 at ¶150.

- (m) **9[l]: providing, via a reporting facility, a composite security rating for the entity based on the internal security rating and the external security rating, wherein at least one of the internal security features or the external security features indicates malicious activity associated with an IP address of the entity.**

See limitation 1[k]. EX1003 at ¶151.

- 9. **Claim 10: The system of claim 9, wherein the one or more computer systems are further programmed to perform operations comprising: determining the composite security rating based on a weighted combination of the internal security rating and the external security rating.**

See claim 2. EX1003 at ¶152.

- 10. **Claim 12: The system of claim 9, wherein the internal security features and the external security features comprise at least one of: a number of remotely exploitable vulnerabilities of the entity; a number of security incidents; or a number of vulnerable versions of software of the entity.**

As discussed above for claim 4, Tippet discloses that the “local vulnerability factor” (i.e. *internal security feature*) comprises *a number of security incidents*. To the extent Patent Owner argues that this claim also requires that the external security features comprise one of the above pieces of information, Tippet discloses that the

“general threat factor components” (*i.e.* ***external security features***) can be derived from “data related to security events [*i.e.* ***security incidents***] that have transpired on the network 228.” EX1006 at ¶37; EX1003 at ¶¶153-54. In addition, Tippet discloses that the general threat factor “represent[s] ... a rate or frequency of security events that threaten the security of information resources.” *Id.* at ¶23. Thus, a POSITA would understand that the rate of security events would include ***a number of security incidents***, since a POSITA would understand that a “rate” is the number of occurrences divided by time. EX1003 at ¶154.

11. **Claim 13: The system of claim 9, wherein each respective transformation function is a normalization of the respective feature, and wherein the one or more computer systems are further programmed to perform operations comprising: when the normalization is applied to two or more of the internal security features or the external security features, summing the normalized features.**

See claim 5. EX1003 at ¶155.

12. **Claim 14: The system of claim 9, wherein determining the internal security rating further comprises weighting the first plurality of transformed features.**

See claim 6. EX1003 at ¶156.

13. **Claim 15: The system of claim 1, wherein combining the first plurality of transformed features further comprises: summing the first plurality of transformed features; and normalizing the summed features by a set of normalization factors.**

See claim 7. EX1003 at ¶157.

- 14. Claim 16: The system of claim 9, wherein combining the second plurality of transformed features further comprises: summing the second plurality of transformed features; and normalizing the summed features by a set of normalization factors.**

See claim 8. EX1003 at ¶158.

B. Ground 2: Tippet, McGovern

Claims 3 and 11 recite that the internal data sources from which information is collected comprise of a number of different types of information. While Tippet discloses several of such information, it does not expressly disclose all of them. However, McGovern discloses collecting information from such data sources to generate a network security assessment. As discussed below, it would have been obvious to combine such teachings with Tippet. EX1003 at ¶159.

1. Motivation to Combine

A POSITA would be motivated to incorporate McGovern’s teachings of collecting various types of information for performing a security assessment of a network. EX1003 at ¶¶160-61.

McGovern teaches a “method for information security assessment” that uses various “security parameters [that] relate to a plurality of aspects of an information system.” EX1007 at ¶29. Such parameters “may encompass the key aspects of information security as described above, such as identity management, vulnerability management, threat management, trust management, and disaster recovery plans” as well as “the basics of an information system, such as hardware and software

configuration, network size and scale, which may also have an impact on security risks.” *Id.* For example, “[v]ulnerability management ... involve[s]... receiving vulnerability updates and applying security patches to software and firmware components” as well as “the use of software tools for security scanning and vulnerability removal.” *Id.* at ¶23. Similarly, “identity and access management” involves information about firewalls and their “implementation of access policies, enforcement of user roles and entitlements, strength of encryption algorithms, and even the availability and quality of directory services.” *Id.* at ¶25. McGovern uses these security parameters to measure “degrees of compliance” which is then quantified and used to perform a security assessment of the network. *Id.* at ¶¶35-37.

As discussed in Ground 1, Tippet discloses generating a “local vulnerability factor” using various types of information “related to the local vulnerability of the information resources associated with the entity.” EX1006 at ¶49. Tippet further discloses that the local vulnerability factor is used to generate a local security risk index which “represent[s] the security” of an entity’s network. EX1006 at ¶46. A POSITA would have been motivated to incorporate McGovern’s teachings of “security parameters,” all of which were well-known and commonly collected information for assessing a network’s security, as additional sources of information to be used with calculating Tippet’s local vulnerability factor. EX1003 at ¶162. Since Tippet discloses that the “local vulnerability factor” uses any information

related to the security vulnerability of the entity, a POSITA would be motivated to give effect to that teaching by using other well-known sources of information about a network's vulnerabilities and security such as those described in McGovern. *Id.* A POSITA would have known that additional sources of information would improve the accuracy of Tippet's local vulnerability factor, as well as its use in generating a local security risk index. *Id.* Indeed, Tippet describes that the local security risk index is "used to certify the security" of the entity's network, which is used to "verify to outside parties such as clients, partners, insurers, vendors, consultants, associates, competitors, or other parties" that the network is secure. EX1006 at ¶62. Thus, a POSITA knowing the importance of the local security vulnerability factor in certifying the entity's network would desire to improve its accuracy and be as comprehensive as possible in assessing all aspects of a network's security, which could be accomplished by making use of the sources of information described by McGovern. EX1003 at ¶162.

Consistent with these teachings in Tippet, McGovern teaches that the "security parameters" can be used to assess "degrees of compliance ... for each security parameter," which "qualitatively and/or quantitatively describe what is in place in an information system with respect to the corresponding security parameter." EX1007 at ¶35. In other words, McGovern expressly teaches that its security parameters are used to assess a network's security, and a POSITA would be

motivated by such teachings to use McGovern’s security parameters as part of calculating Tippet’s local vulnerability factor. EX1003 at ¶163.

A POSITA would have had a reasonable expectation of success in combining Tippet and McGovern. EX1003 at ¶164. McGovern provides detailed descriptions on the types of information that is collected for each “security parameter,” which were information that was well-known and well-within the skill of an ordinary artisan to implement within a conventional network. *Id.* In addition, McGovern also explains that the security parameters can be “quantif[ied] ... to ultimately reach an overall risk assessment,” which would be compatible with Tippet’s teachings of normalizing and weighing the local vulnerability factor components into a quantifiable amount to be used to calculate the local security risk index. EX1007 at ¶36; EX1006 at ¶47; EX1003 at ¶164.

Finally, Tippet and McGovern are analogous art to the ’976 patent because all three describe performing security assessments of a network. EX1001 at Abstract (“A method and system for creating a composite security rating from security characterization data of a third party computer system.”); EX1006 at Abstract (“A system and method for assessing the risk to information resources that may include the generation and/or use of a security risk index.”); EX1007 at Abstract (“Methods for information security assessment and data risk scoring are disclosed.”); EX1003 at ¶165.

2. **Claim 3: The method of claim 1, wherein the plurality of internal data sources comprises: vulnerability scan data of the entity; data indicating firewall rules of the entity; data from security incident reports corresponding to the entity; data indicative of computer network configurations of the entity; data indicative of software inventory of the entity; data indicative of security policies of the entity; data indicative of security controls of the entity; and data indicative of user behavior corresponding to the entity.**

Tippett and McGovern together disclose each of the claimed *internal data sources*. EX1003 at ¶166. As discussed above, it would have been obvious to combine Tippett and McGovern.

“vulnerability scan data of the entity”: McGovern discloses that information about “vulnerability management” is collected to perform an information security assessment. EX1007 at ¶¶28-29. According to McGovern, “[v]ulnerability management ... involve[s] ... the use of software tools for *security scanning and vulnerability removal*.” *Id.* at ¶23. McGovern also discloses collecting information related to “virus scan logs.” *Id.* at ¶60. Such information is *vulnerability scan data of the entity*, including “virus scan logs,” since a POSITA would understand that viruses typically exploit network and entity vulnerabilities. EX1003 at ¶167.

McGovern further discloses that such information is collected by “data sources” that “include *internal* data records maintained by the organization,” *i.e.* *internal data sources*. EX1003 at ¶168.

“data indicating firewall rules of the entity”: McGovern discloses that information about “identity management” is collected to perform an information security assessment. EX1007 at ¶¶28-29. According to McGovern, “identity and access management” of “firewall[s]” involves “implementation of access policies, enforcement of user roles and entitlements, strength of encryption algorithms, and even the availability and quality of directory services.” *Id.* at ¶25. Such information is ***data indicating firewall rules of the entity*** because it is indicative of firewall rules and policies related to access, user roles and permissions, and encryption algorithms. EX1003 at ¶169.

McGovern further discloses that such information is collected by “data sources” that “include ***internal*** data records maintained by the organization,” *i.e.* ***internal data sources***. EX1003 at ¶170.

“data from security incident reports corresponding to the entity”: Tippet discloses that information about the entity’s “a past history of at least one type of security breach” is collected from ***internal data sources***. EX1006 at ¶49. Such information is ***data from security incident reports*** since a security breach is a ***security incident*** and the past history of security breach will include ***reports*** of such incidents. EX1003 at ¶171.

“data indicative of computer network configurations of the entity”: McGovern discloses that information about “hardware and software configuration”

and “network size and scale” is collected to perform an information security assessment. EX1007 at ¶¶28-29. Such information is ***data indicative of computer network configurations of the entity*** because it is indicative of how the network is configured in terms of the hardware and software configuration of its network nodes as well as its configuration with respect to size and scale. EX1003 at ¶172.

McGovern further discloses that such information is collected by “data sources” that “include ***internal*** data records maintained by the organization,” *i.e.* ***internal data sources***. EX1003 at ¶173.

“data indicative of software inventory of the entity”: McGovern discloses that information about “vulnerability management” is collected to perform an information security assessment. EX1007 at ¶¶28-29. According to McGovern, “[v]ulnerability management ... involve[s]... receiving vulnerability updates and applying security patches to software and firmware components” as well as “the use of software tools for security scanning and vulnerability removal.” *Id.* at ¶23. Such information is ***data indicative of software inventory of the entity*** because it is indicative of the inventory of software patches and software tools installed on an entity’s network. EX1003 at ¶174.

McGovern further discloses that such information is collected by “data sources” that “include ***internal*** data records maintained by the organization,” *i.e.* ***internal data sources***. EX1003 at ¶175.

“data indicative of security policies of the entity”: Tippet discloses that information about a “mitigating measure designed to secure information resources” and “a future plan for securing the information resources associated with the entity” are collected from ***internal data sources***. EX1006 at ¶49. Such information is ***data indicative of security policies of the entity*** since they reflect the entity’s policy on mitigating security events and securing the entity’s information resources. EX1003 at ¶176.

“data indicative of security controls of the entity”: Tippet discloses that information about a “mitigating measure designed to secure information resources” is collected from ***internal data sources***. EX1006 at ¶49. Tippet further discloses that mitigation includes “deterrence,” “protection,” “detection,” and “recovery.” *Id.* at ¶52. Thus, such information is ***data indicative of security controls of the entity*** since it reflects how the entity controls its information sources to deter or protect from security events. EX1003 at ¶177.

“data indicative of user behavior corresponding to the entity”: McGovern discloses that information about “identity management” is collected to perform an information security assessment. EX1007 at ¶¶28-29. According to McGovern, information about “identity management” includes “how often a network user is required to change his or her login password.” *Id.* at ¶36. Such information is ***data indicative of user behavior corresponding to the entity*** because it is indicative of

how often users within the entity’s network change their passwords. EX1003 at ¶178.

McGovern also discloses collecting information “corresponding to ... authorized users” and “attempted unauthorized logins.” EX1007 at ¶38. Such information is also *data indicative of user behavior corresponding to the entity* because it is indicative of login behaviors for users belonging to the entity or attempting to gain access to entity. EX1003 at ¶179.

McGovern further discloses that such information is collected by “data sources” that “include *internal* data records maintained by the organization,” *i.e. internal data sources*. EX1003 at ¶180.

3. **Claim 11: The system of claim 9, wherein the plurality of internal data sources comprises: vulnerability scan data of the entity; data indicating firewall rules of the entity; data from security incident reports corresponding to the entity; data indicative of computer network configurations of the entity; data indicative of software inventory of the entity; data indicative of security policies of the entity; data indicative of security controls of the entity; and data indicative of user behavior corresponding to the entity.**

See claim 3. EX1003 at ¶181.

VIII. MANDATORY NOTICES AND FEES

A. Real Party-In-Interest

The real party-in-interest is Normshield Inc. d/b/a Black Kite Inc.

B. Related Matters

To the best of Petitioner's knowledge, the '976 patent is asserted in the district court case *BitSight Technologies, Inc. v. NormShield Inc.*, 1:23-cv-12055 (D. Mass.)

C. Counsel and Service Information

Petitioner provides the following counsel and service information.

Petitioner consents to electronic service the email addresses listed in the table below. Pursuant to 37 C.F.R. § 42.10(b), Power of Attorney accompany this Petition.

LEAD COUNSEL	BACK-UP COUNSEL
James M. Glass (Reg. No. 46729) jimglass@quinnemanuel.com QUINN EMANUEL URQUHART & SULLIVAN, LLP 51 Madison Avenue, 22 nd Floor New York, NY 10010 Tel: (212) 849-7000 Fax: (212) 849-7100	David Elihu (Reg. No. 65,717) davideliu@quinnemanuel.com QUINN EMANUEL URQUHART & SULLIVAN, LLP 865 S. Figueroa St., 10th Floor Los Angeles, California 90017 Tel : (213) 443-3000 Fax : (213) 443-3000 Quincy Lu (Reg. No. 76,954) quincylu@quinnemanuel.com QUINN EMANUEL URQUHART & SULLIVAN, LLP 1109 First Avenue, Suite 210 Seattle, WA 98101 Tel: (206) 905-7000 Fax: (206) 905-7100 Brett Watkins (Reg. No. 60,458) brettwatkins@quinnemanuel.com

	QUINN EMANUEL URQUHART & SULLIVAN, LLP 700 Louisiana St., Suite 3900 Houston, TX 77002 Tel: (713) 221-7000 Fax: (713) 221-7100 Andrew Bramhall (<i>pro hac vice</i> forthcoming) andrewbramhall@quinnemanuel.com QUINN EMANUEL URQUHART & SULLIVAN, LLP 555 Twin Dolphin Dr., 5th Floor Redwood Shores, California 94065 Tel: (650) 801-5000 Fax: (650) 801-5100
--	---

D. Payment of Fees

The undersigned authorizes the Office to charge the fee required for this Petition for *Inter Partes* Review to Deposit Account No. 50-5708. Any additional fees that might be due are also authorized.

Date: December 10, 2024

Respectfully submitted,

By: /s/ James M. Glass
James M. Glass

Counsel for Petitioner

**CERTIFICATE OF COMPLIANCE WITH
TYPE-VOLUME LIMITATION, TYPEFACE REQUIREMENTS,
AND TYPE STYLE REQUIREMENTS**

1. This Petition complies with the type-volume limitation of 14,000 words, comprising 9,497 words, as counted using the Microsoft Word software that was used to prepare this paper, excluding the parts exempted by 37 C.F.R. § 42.24(a).

2. This Petition complies with the general format requirements of 37 C.F.R. § 42.6(a) and has been prepared using Microsoft® Word 2016 in 14-point Times New Roman.

Date: December 10, 2024

By: /s/ James M. Glass
James M. Glass
QUINN EMANUEL URQUHART
& SULLIVAN, LLP
51 Madison Avenue, 22nd Floor
New York, NY 10010
Tel: (212) 849-7000
Fax: (212) 849-7100

Counsel for Petitioner

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on December 10, 2024, true and correct copies of the foregoing document and supporting materials were served in its entirety on the Patent Owner at the following address of record as listed on PAIR via Priority Mail Express® or Express Mail:

GOODWIN PROCTER LLP
Patent Administrator
100 Northern Avenue
Boston, MA 02210
United States

Official Correspondence Address

Courtesy copies were also sent via electronic mail to Patent Owner's counsel of record in the related district court proceeding

Douglas J. Kline
Goodwin Procter, LLP
100 Northern Avenue
Boston, MA 02210
617-570-1000
Email: dkline@goodwinlaw.com
ATTORNEY TO BE NOTICED

Kelly Grosshuesch
Goodwin Procter LLP
1900 N Street, N.W.
Washington, DC 20036
202-346-4000
Fax: 202-346-4444
Email: KGrosshuesch@goodwinlaw.com
ATTORNEY TO BE NOTICED

Naomi Birbach
Goodwin Procter LLP
The New York Times Building
620 Eighth Avenue
New York City, NY 10018

212-459-7374

Email: nbirbach@goodwinlaw.com

ATTORNEY TO BE NOTICED

Robert D. Carroll

Goodwin Procter, LLP

100 Northern Avenue

Boston, MA 02210

617-570-1000

Fax: 617-523-1231

Email: rcarroll@goodwinlaw.com

ATTORNEY TO BE NOTICED

Timothy Keegan

Goodwin Procter LLP

620 Eighth Avenue

New York, NY 10018

212-459-7022

Email: tkeegan@goodwinlaw.com

ATTORNEY TO BE NOTICED

Date: December 10, 2024

By: /s/ James M. Glass

James M. Glass

QUINN EMANUEL URQUHART
& SULLIVAN, LLP

51 Madison Avenue, 22nd Floor

New York, NY 10010

Tel: (212) 849-7000

Fax: (212) 849-7100

Counsel for Petitioner