

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

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

v.

BITSIGHT TECHNOLOGIES, INC.,
Patent Owner

Case IPR2024-01392
Patent 10,805,331

**DECLARATION OF KEVIN C. ALMEROOTH, PH.D. IN SUPPORT OF
PETITION FOR INTER PARTES REVIEW OF
UNITED STATES PATENT NO. 10,805,331**

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
II.	BACKGROUND AND QUALIFICATIONS	2
III.	LEGAL STANDARDS.....	14
	A. Obviousness	14
	B. Claim Construction	19
IV.	PERSON OF ORDINARY SKILL IN THE ART AND THE TIME OF THE ALLEGED INVENTION.....	20
V.	THE '331 patent.....	21
	A. Technical Background	21
	B. Description of the '331 Patent's Specification	34
	C. The '331 Patent's Prosecution History	34
	D. Interpretation of the '331 patent's Challenged Claims	36
VI.	PUBLIC AVAILABILITY OF CERTAIN EXHIBITS	37
	A. McNab.....	37
	B. Internet Archive Pages.....	38
	C. Public Videos	39
VII.	GROUND 1: Tippet, McNab and McGovern RENDER OBVIOUS CLAIMS 1-29	41
	A. Rationale to Combine	41
	1. McNab.....	42
	2. McGovern	46
	B. Claim 1	50
	1. 1[pre], 1[a]: A method comprising: collecting information about two or more organizations that have computer systems, network resources, and employees, the organizations posing risks through business relationships of the organizations with other parties,.....	50

2.	1[b]: the information collected about the organizations being indicative of compromises, vulnerabilities or configurations of technology systems of the organizations and indicative of resiliencies of the organizations to recover from such compromises, vulnerabilities or configurations, ...	52
3.	1[c]: the information indicative of durations of events associated with compromises or vulnerabilities or configurations, ...	56
4.	1[d]: at least some of the information about each of the organizations being collected automatically by computer using sensors on the Internet, ...	58
5.	1[e]: the information about each of the organizations being collected from two or more sources, one or more of the sources not being controlled by the organization, the information from at least the one or more sources that are not controlled by the organization being collected without permission of the organization, ...	62
6.	1[f]: at least partly automatically gathering information about assets that each of the organizations owns, controls, uses, or is affiliated with, including IP addresses and IP network address ranges, computer services residing within address ranges, or domain names, ...	65
7.	1[g]: at least one of the sources for each of the organizations comprising a public source or a commercial source, ...	67
8.	1[h]: processing by computer the information from the two or more sources for each of the organizations to form a composite rating of the organization that is indicative of a degree of risk to the organization or to a party through a business relationship with the organization, the composite rating comprising a calculated composite of metrics and data derived or collected from the sources, ...	67
9.	1[i]: the processing comprising applying transformations to the data and metrics, and the processing comprising applying weights to the data and the metrics, ...	70
10.	1[j]: the metrics including a measure of the extent of, the frequency of, or duration of compromise of the technology systems of the organization, or of a configuration or vulnerability of the organization, and a measure of the resilience of the organization to recover from such vulnerability, the measure of the resilience being inversely proportional to the duration of detected malicious activity, and.....	71

11.	1[k]: in connection with assessing a business risk to the organization or to a party through a business relationship with at least one of the organizations, delivering reports of the composite ratings of the organizations through a reporting facility to enable users of the reporting facility to monitor, assess, and mitigate the risks, based on the security vulnerabilities and resiliencies, in doing business with the organization and to compare the composite ratings of the organizations.	72
C.	Claim 2: The method of claim 1, wherein the collected information is represented by at least two data types. Claim 3: The method of claim 2, wherein the at least two data types include at least one of breach disclosures, block lists, configuration parameters, an identification of malware servers, an identification of a reputation, an identification of suspicious activity, an identification of spyware, white lists, an identification of compromised hosts, an identification of malicious activity, an identification of spam activity, an identification of vulnerable hosts, an identification of phishing activity, or an identification of e-mail viruses.	75
D.	Claim 4: The method of claim 1, wherein the collected information evidences internal security controls.	76
E.	Claim 5: The method of claim 1, wherein the collected information comprises outcomes of each of the organizations.	77
F.	Claim 6: The method of claim 1, wherein the collected information evidences operational execution of security measures of each of the organizations.	77
G.	Claim 7: The method of claim 1, wherein the collected information indicates whether a computer system of each of the organizations served malicious code to another system.	78
H.	Claim 8: The method of claim 1, wherein the collected information indicates whether a computer system of each of the organizations communicated with a known attacker controlled network or sensor outside the control or network of the organization.	79
I.	Claim 9: The method of claim 1, comprising: forming a series of the security ratings of each of the organizations. Claim 10: The method of claim 9, comprising: determining a trend from the series of ratings. Claim 11: The method of claim 9, comprising displaying the series of composite ratings.	80
J.	Claim 12: The method of claim 11, wherein displaying the series of composite ratings for each of the organizations comprises posting the series of composite ratings for the organization to a web portal.	82

K.	Claim 13: The method of claim 1, wherein the collected information represents externally observable outcome information.	83
L.	Claim 14: The method of claim 1, comprising: determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information.....	83
M.	Claim 15: The method of claim 1, wherein: the collected information comprises at least two security characterizations of a computer system of each of the organizations.	84
N.	Claim 16: The method of claim 1, wherein the collected information comprises a characterization of behavior of an employee of at least one of the organizations.	85
O.	Claim 17: The method of claim 1, wherein the collected information comprises characterizations other than characterizations about a computer system of at least one of the organizations.	85
P.	Claim 18: The method of claim 1, wherein the collected information comprises characterizations about policies of at least one of the organizations.	87
Q.	Claim 19: The method of claim 1, wherein the collected information comprises characterizations about information technology assets that at least one of the organizations owns, controls, uses, or is affiliated with.....	87
R.	Claim 20: The method of claim 1 in which collected information represents: (a) physical states, (b) technical states, (c) organizational states, or (d) cultural states of at least one of the organizations which can be exploited to create a security breach; or (e) the organization's ability to recover from a security breach; or any combination of two or more of these.....	87
S.	Claim 21: The method of claim 1 in which processing the information to form a composite rating comprises correlating data across the sources of information.....	88
T.	Claim 22: The method of claim 1 in which processing the information to form a composite rating comprises statistically correlating the composite rating with actual outcomes.	88
U.	Claim 23: The method of claim 1 in which the vulnerability comprises physical, technical, organizational, or cultural states that can be exploited to create a security breach.	89
V.	Claim 24.....	89
1.	24[pre]: A method comprising:.....	89

2.	24[a]: collecting, from at least two sources, information about two or more organizations, the collected information representing at least two data types, the collected information comprising outcomes of each of the organizations, ...	89
3.	24[b]: at least some of the information for each of the organizations being collected automatically by computer from at least two sources, one or more of the sources not controlled by the organization, ...	90
4.	24[c]: the information from at least the one or more sources that are not controlled by the organization being collected without permission of the organization, at least one of the sources including a commercial data source, ...	91
5.	24[d]: processing the information from both of the two sources for each of the organizations to form a composite rating of a security vulnerability of the organization and of a resilience of the organization to recover from a security breach, the resilience being inversely proportional to the duration of detected malicious activity, the processing including applying models that account for differences in the respective sources, ...	91
6.	24[e]: normalizing the composite rating of each of the organizations based on a size characteristic of the organization to enable comparisons of composite ratings between the two or more organizations, ...	93
7.	24[f]: forming a series of the security ratings of each of the organizations, determining a trend from the series of ratings, and displaying the series of composite ratings through a portal, ...	94
8.	24[g]: determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information, and	95
9.	24[h]: reporting the composite ratings of the organizations through a portal to enable customers to monitor, assess, and mitigate risk in doing business with the organizations and to compare the composite ratings across the organizations.	95
W.	Claim 25: The system of claim 24, determining a confidence range of the composite rating, the size of the range varying inversely with the level of confidence in the composite rating.	95
X.	Claim 26: The system of claim 25, wherein the confidence range is based on redundancy of the security characterizations.	97

Y.	Claim 27: The system of claim 25, wherein the confidence range is based on a size of the third party computer system.	97
Z.	Claim 28: The method of claim 1 comprising ranking the organization and other organizations within sectors or peer-groups or globally.....	98
AA.	Claim 29.....	100
1.	29[pre]: A method comprising:.....	100
2.	29[a]: collecting information about an organization that has computer systems, network resources, and employees, the organization posing risks to itself or to other parties through business relationships of the organization with the other parties, ...	100
3.	29[b]: the information collected about the organization including (a) information collected automatically by computer on the Internet without permission of the organization, and (b) information indicative of resiliencies of the organization to recover from a security breach associated with a compromise or a vulnerability, the resiliencies being inversely proportional to the duration of detected malicious activity, ...	100
4.	29[c]: processing the information by computer to form a composite rating of the organization that is indicative of a degree of risk based on a business relationship with the organization, the composite rating comprising a measure of the resiliencies of the organization to recover from a security breach, and.....	101
5.	29[d]: in connection with assessing the degree of risk, delivering a report of the composite rating of the organization through a reporting facility to enable a user of the reporting facility to assess the risks, based at least in part on the resiliencies.....	101
VIII.	CONCLUSION	102

I. INTRODUCTION

1. I have been retained by Normshield Inc. d/b/a Black Kite Inc. (“Petitioner”) as an independent expert consultant in this proceeding before the United States Patent and Trademark Office (“PTO”) against BitSight Technologies, Inc. (“Patent Owner”) regarding U.S. Patent No. 10,805,331 (“the ’331 patent”) (Ex. 1001).¹ I have been asked to submit this Declaration on behalf of Petitioner.

2. I have been asked to consider whether certain references disclose or render obvious the features recited in claims 1-29 (collectively, the “Challenged Claims”) of the ’331 patent. My opinions are set forth below. Based on my experience and expertise, it is my opinion that the prior art renders obvious all limitations of the Challenged Claims, as I discuss in detail below.

3. I am being compensated at a rate of \$850 per hour for my work in this proceeding. My compensation is in no way contingent on the nature of my findings, the presentation of my findings in testimony, or the outcome of this or any other proceeding. I have no other interest in this proceeding.

4. All of my opinions stated in this Declaration are based on my own personal knowledge and professional judgment. I am over 18 years of age and, if I am

¹ Where appropriate, I refer to exhibits that I understand are to be attached to the petition for *Inter Partes* Review of the ’331 patent.

called upon to do so, I would be competent to testify as to the matters set forth in this Declaration.

II. BACKGROUND AND QUALIFICATIONS

5. I am currently a Professor Emeritus in the Department of Computer Science at the University of California, Santa Barbara (UCSB). While at UCSB, I held faculty appointments and was a founding member of the Computer Engineering (CE) Program, Media Arts and Technology (MAT) Program, and the Technology Management Program (TMP). I also served as the Associate Director of the Center for Information Technology and Society (CITS) from 1999 to 2012. I have been a faculty member at UCSB since July 1997.

6. I hold three degrees from the Georgia Institute of Technology: (1) a Bachelor of Science degree in Information and Computer Science (with minors in Economics, Technical Communication, and American Literature) earned in June 1992; (2) a Master of Science degree in Computer Science (with specialization in Networking and Systems) earned in June 1994; and (3) a Doctor of Philosophy (Ph.D.) degree in Computer Science (Dissertation Title: Networking and System Support for the Efficient, Scalable Delivery of Services in Interactive Multimedia System, minor in Telecommunications Public Policy) earned in June 1997. During my education, I took a wide variety of courses as demonstrated by my minor. My undergraduate degree also

included a number of courses more typical of a degree in electrical engineering including digital logic, signal processing, and telecommunications theory.

7. One of the major concentrations of my research over the past 30+ years has been the delivery of multimedia content and data between computing devices, including through various network architectures. In my research, I have studied large-scale content delivery systems, and the use of servers located in a variety of geographic locations to provide scalable delivery to hundreds or thousands of users simultaneously. I have also studied smaller-scale content delivery systems in which content is exchanged between individual computers and portable devices. My work has emphasized the exchange of content more efficiently across computer networks, including the scalable delivery of content to many users, mobile computing, satellite networking, delivering content to mobile devices, and network support for data delivery in wireless networks.

8. In 1992, the initial focus of my research was on the provision of interactive functions (e.g., VCR-style functions like pause, rewind, and fast-forward) for near video-on-demand systems in cable systems; in particular, how to aggregate requests for movies at a cable head-end and then how to satisfy a multitude of requests using one audio/video stream broadcast to multiple receivers simultaneously. This research has continually evolved and resulted in the development of techniques to scalably deliver on-demand content, including audio, video, web documents, and other

types of data, through the Internet and over other types of networks, including over cable systems, broadband telephone lines, and satellite links.

9. An important component of my research has been investigating the challenges of communicating multimedia content, including video, between computers and across networks including the Internet. Although the early Internet was used mostly for text-based, non-real time applications, the interest in sharing multimedia content, such as video, quickly developed. Multimedia-based applications ranged from downloading content to a device to streaming multimedia content to be instantly used. One of the challenges was that multimedia content is typically larger than text-only content, but there are also opportunities to use different delivery techniques since multimedia content is more resilient to errors. I have worked on a variety of research problems and used a number of systems that were developed to deliver multimedia content to users. One content-delivery method I have researched is the one-to-many communication facility called “multicast,” first deployed as the Multicast Backbone, a virtual overlay network supporting one-to-many communication. Multicast is one technique that can be used on the Internet to provide streaming media support for complex applications like video-on-demand, distance learning, distributed collaboration, distributed games, and large-scale wireless communication. The delivery of media through multicast often involves using Internet infrastructure, devices and protocols, including protocols for routing and TCP/IP.

10. Starting in 1997, I worked on a project to integrate the streaming media capabilities of the Internet together with the interactivity of the web. I developed a project called the Interactive Multimedia Jukebox (IMJ). Users would visit a web page and select content to view. The content would then be scheduled on one of a number of channels, including delivery to students in Georgia Tech dorms delivered via the campus cable plant. The content of each channel was delivered using multicast communication.

11. In the IMJ, the number of channels varied depending on the capabilities of the server including the available bandwidth of its connection to the Internet. If one of the channels was idle, the requesting user would be able to watch their selection immediately. If all channels were streaming previously selected content, the user's selection would be queued on the channel with the shortest wait time. In the meantime, the user would see what content was currently playing on other channels, and because of the use of multicast, would be able to join one of the existing channels and watch the content at the point it was currently being transmitted.

12. The IMJ service combined the interactivity of the web with the streaming capabilities of the Internet to create a jukebox-like service. It supported true Video-on-Demand when capacity allowed, but scaled to any number of users based on queuing requested programs. As part of the project, we obtained permission from Turner Broadcasting to transmit cartoons and other short-subject content. We also

connected the IMJ into the Georgia Tech campus cable television network so that students in their dorms could use the web to request content and then view that content on one of the campus's public access channels.

13. More recently, I have also studied issues concerning how users choose content, especially when considering the price of that content. My research has examined how dynamic content pricing can be used to control system load. By raising prices when systems start to become overloaded (i.e., when all available resources are fully utilized) and reducing prices when system capacity is readily available, users' capacity to pay as well as their willingness can be used as factors in stabilizing the response time of a system. This capability is particularly useful in systems where content is downloaded or streamed on-demand to users.

14. As a parallel research theme, starting in 1997, I began researching issues related to wireless devices and sensors. In particular, I was interested in showing how to provide greater communication capability to "lightweight devices," i.e., small form-factor, resource-constrained (e.g., CPU, memory, networking, and power) devices. Starting in 1998, I published several papers on my work to develop a flexible, lightweight, battery-aware network protocol stack. The lightweight protocols we envisioned were similar in nature to protocols like Bluetooth, Universal Plug and Play (UpnP) and Digital Living Network Alliance (DLNA).

15. From this initial work, I have made wireless networking—including ad hoc, mesh networks and wireless devices—one of the major themes of my research. My work in wireless networks spans the protocol stack from applications through to the encoding and exchange of data at the data link and physical layers.

16. At the application layer, even before the large-scale “app stores” were available, my research looked at building, installing, and using apps for a variety of purposes, from network monitoring to support for traditional computer-based applications (e.g., content retrieval) to new applications enabled by ubiquitous, mobile devices. For example, my research has looked at developing applications for virally exchanging and tracking “coupons” through “opportunistic contact” among mobile wireless devices (i.e., communication among devices moving into communication range with each other). In many of the courses I have taught there is a project component. Through these projects I have supervised numerous efforts to develop new “apps” for download and use across a variety of mobile platforms.

17. Toward the middle of the protocol stack, my research has also looked to build wireless infrastructure support to enable communication among a set of mobile devices unaided by any other kind of network infrastructure. These kinds of networks are useful either in challenged network environments (e.g., when a natural disaster has destroyed existing infrastructure) or when suitable support for network communication never existed. The deployment of such networks (or even the use of traditional network

support) are critical to support services like disaster relief, catastrophic event coordination, and emergency services deployment.

18. Yet another theme is monitoring wireless networks, in particular different variants of IEEE 802.11 compliant networks, to (1) understand the operation of the various protocols used in real-world deployments, (2) use these measurements to characterize use of the networks and identify protocol limitations and weaknesses, and (3) propose and evaluate solutions to these problems. I have successfully used monitoring techniques to study wireless data link layer protocol operation and to improve performance by enhancing the operation of such protocols. For wireless protocols, this research includes functions like network acquisition and channel bonding.

19. One theme in my wireless network research has been cross-layer solutions and innovations. As mentioned above, with greater wireless device use and network support, we envisioned new application paradigms and services, for example, when mobile devices come into contact with each other. Instead of relying on existing infrastructure to relay communication, the devices are able to discover each other and communicate directly. Other examples include discovering and using location information to enhance users' experiences. Network support and novel applications span use a variety of network architectures supporting users on foot, in vehicles, and across varying terrains and environments. Finally, we studied how communication

efficiency can be supported through intelligent handoffs as well as location and movement prediction.

20. Protecting networks, including their operation and content, has been an underlying theme of my research almost since the beginning of my research career. Starting in 2000, I have been involved in several projects that specifically address security, network protection, and firewalls. After significant background work, a team on which I was a member successfully submitted a \$4.3M grant proPOSITAl to the Army Research Office (ARO) at the Department of Defense to propose and develop a high-speed intrusion detection system. Key aspects of the system included associating streams of packets and analyzing them for viruses and other malware. Once the grant was awarded, we spent several years developing and meeting the milestones of the project. A number of my students worked on related projects and published papers on topics ranging from intrusion detection to developing advanced techniques to be incorporated into firewalls. I have also used firewalls, including their associated malware detection features, in developing techniques for the classroom to ensure that students are not distracted by online content.

21. My recent work ties some of the various threads of my past research together. I have investigated content delivery in online social networks and proposed reputation management systems in large-scale social networks and marketplaces. On the content delivery side, I have looked at issues of caching and cache placement,

especially when content being shared and the cache has geographical relevance. We were able to show that effective caching strategies can greatly improve performance and reduce deployment costs. Our work on reputation systems showed that reputations have economic value, and as such, creates a motivation to manipulate reputations. In response, we developed a variety of solutions to protect the integrity of reputations in online social networks. The techniques we developed for content delivery and reputation management were particularly relevant in peer-to-peer communication and recommendations for downloadable “apps.”

22. As an important component of my research program, I have been involved in the development of academic research into available technology in the market place. One aspect of this work is my involvement in the Internet Engineering Task Force (IETF). The IETF is a large and open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. I have been involved in various IETF groups including many content delivery-related working groups like the Audio Video Transport (AVT) group, the MBone Deployment (MBONED) group, Source Specific Multicast (SSM) group, the Inter-Domain Multicast Routing (IDMR) group, the Reliable Multicast Transport (RMT) group, the Protocol Independent Multicast (PIM) group, etc. I have also served as a member of the Multicast Directorate (MADDOGS), which oversaw the standardization of all things related to multicast in

the IETF. Finally, I was the Chair of the Internet2 Multicast Working Group for seven years.

23. My involvement in the research community extends to leadership positions for several academic journals and conferences. I am the co-chair of the Steering Committee for the ACM Network and System Support for Digital Audio and Video (NOSSDAV) workshop and on the Steering Committees for the International Conference on Network Protocols (ICNP), ACM Sigcomm Workshop on Challenged Networks (CHANTS), and IEEE Global Internet (GI) Symposium. I have served or am serving on the Editorial Boards of IEEE/ACM Transactions on Networking, IEEE Transactions on Mobile Computing, IEEE Network, ACM Computers in Entertainment, AACE Journal of Interactive Learning Research (JILR), and ACM Computer Communications Review. I have co-chaired a number of conferences and workshops including the IEEE International Conference on Network Protocols (ICNP), IEEE Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), International Conference on Communication Systems and Networks (COMSNETS), IFIP/IEEE International Conference on Management of Multimedia Networks and Services (MMNS), the International Workshop On Wireless Network Measurement (WiNMee), ACM Sigcomm Workshop on Challenged Networks (CHANTS), the Network Group Communication (NGC) workshop, and the Global

Internet Symposium, and I have served on the program committees for numerous conferences.

24. Furthermore, in the courses I taught at UCSB, a significant portion of my curriculum covered aspects of the Internet and network communication including the physical and data link layers of the Open System Interconnect (OSI) protocol stack, and standardized protocols for communicating across a variety of physical media such as cable systems, telephone lines, wireless, and high-speed Local Area Networks (LANs). The courses I have taught also cover most major topics in Internet communication, including data communication, multimedia encoding, and mobile application design. My research and courses have covered a range of physical infrastructures for delivering content over networks, including cable, Integrated Services Digital Network (ISDN), Ethernet, Asynchronous Transfer Mode (ATM), fiber, and Digital Subscriber Line (DSL). For a complete list of courses I have taught, see my curriculum vitae (CV).

25. In addition, I co-founded a technology company called Santa Barbara Labs that was working under a sub-contract from the U.S. Air Force to develop very accurate emulation systems for the military's next generation internetwork. Santa Barbara Labs' focus was in developing an emulation platform to test the performance characteristics of the network architecture in the variety of environments in which it was expected to operate, and, in particular, for network services including Ipv6,

multicast, Quality of Service (QoS), satellite-based communication, and security. Applications for this emulation program included communication of a variety of multimedia-based services, including video conferencing and video-on-demand.

26. In addition to having co-founded a technology company myself, I have worked for, consulted with, and collaborated with companies for nearly 30 years. These companies range from well-established companies to start-ups and include IBM, Hitachi Telecom, Turner Broadcasting System (TBS), Bell South, Digital Fountain, RealNetworks, Intel Research, Cisco Systems, and Lockheed Martin.

27. Through my graduate education, leadership with CITS, involvement in TMP, role in the development of the Internet2 infrastructure, and consulting with ISPs, I have gained a strong understanding in the role of the Internet in our society and the challenges of deploying large-scale production networking infrastructure. CITS, since its inception, has looked at the role of the Internet in society, including how the evolution of technology have created communication opportunities and challenges, including, for example through disruptive technologies like P2P. TMP looks to focus on non-purely technical issues, including, for example, state-of-the-art business methods, strategies for successful technology commercialization, new venture creation, and best practices for fostering innovation. Through my industry collaborations and Internet2 work, I have developed significant experience in the challenges of deploying, monitoring, managing, and scaling communication

infrastructure to support evolving Internet services like streaming media, conferencing, content exchange, social networking, and e-commerce.

28. I am a Member of the Association of Computing Machinery (ACM) and a Fellow of the Institute of Electrical and Electronics Engineers (IEEE).

29. Additional details about my employment history, fields of expertise, courses taught, and publications are further included in my CV attached as Ex. 1004.

30. Based on my professional experience, I believe I am qualified to testify as an expert on matters related to the patent at issue.

III. LEGAL STANDARDS

31. Petitioner' attorneys have explained to me the legal standards that apply in this case. My understanding of those standards is described below. I am not an attorney, and I do not have formal training in the law regarding patents. I have used my understanding of the following legal principles set forth in this section in reaching my opinions.

32. I understand that, in this proceeding, Petitioner have the burden of proving that the challenged claims are invalid by a preponderance of the evidence.

A. Obviousness

33. I have been informed that a claim is invalid as obvious under 35 U.S.C. § 103 (pre-AIA) if the differences between the claimed subject matter and the prior art are such that the subject matter as a whole would have been obvious at the time of the

invention to a person of ordinary skill in the art. I have been informed that the following matters are relevant to determining whether the claimed invention would have been obvious: (1) the scope and content of the prior art, (2) the difference or differences between the patent claim and the prior art, (3) the level of ordinary skill in the art at the time the invention of the patent, and (4) any secondary considerations or objective indicia of non-obviousness.

34. I have been informed that the combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results. When a claim simply arranges prior art elements with each performing the same function it had been known to perform and yields no more than one would expect from such an arrangement, then such a combination is obvious. When a patent claims a structure already known in the prior art altered by the mere substitution of one element for another known in the field, the combination is likely to be obvious unless the combination yields an unpredictable result.

35. I have been informed that when a work is available in one field of endeavor, design incentives and other market forces can prompt variations of it, either in the same field or a different one. If a person of ordinary skill in the art can implement a predictable variation, such a variation is likely unpatentable. For the same reason, if a technique has been used to improve one device, and one of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the

technique is obvious unless its actual application is beyond his or her skill. One question to consider is whether the improvement is more than predictably using prior art elements according to their established functions.

36. I have been informed that it may often be necessary, in a validity analysis, to consider whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue. This can be accomplished by looking to interrelated teachings of multiple patents or other publications or pieces of prior art; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by one of ordinary skill in the art.

37. I have been informed that a validity analysis need not seek out precise teachings directed to the specific subject matter of the challenged claim; it is appropriate to take account of the inferences and creative steps that a person of ordinary skill in the art would employ. I have been informed that a person of ordinary skill in the art is a person of ordinary creativity, not an automaton.

38. I have been informed that a claim composed of several elements is not proved obvious merely by demonstrating that each element was, independently, known in the prior art. I have been informed that it can be important to identify a reason that would have prompted a person of ordinary skill in the art in the relevant field to combine the elements in the way the claimed new invention does. I am told that one

way that subject matter can be proved obvious is by noting there existed at the time of the invention a known problem for which there was an obvious solution encompassed by the patent's claims. I have been informed that any need or problem known in the field of endeavor at the time of the claimed invention and addressed by the patent can provide a reason for combining the elements in the manner claimed.

39. I have been informed that one should not assume that a person of ordinary skill in the art attempting to solve a problem will be led only to those elements of prior art designed to solve the same problem. Instead, I have been informed that since familiar items may have obvious uses beyond their primary purposes, in many cases a person of ordinary skill in the art will be able to fit the teachings of multiple prior art references together like pieces of a puzzle.

40. I have been informed that, when there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, persons of ordinary skill in the art have good reason to pursue the known options within their technical grasp. If this leads to the anticipated success, the product was likely not accomplished by innovation but by using ordinary skill and common sense. I have been informed that, in such an instance, the fact that the combination was obvious to try may show that the combination was obvious.

41. I have been informed that, when determining whether a claimed combination would have been obvious, the correct analysis is not whether a person of

ordinary skill in the art, writing on a blank slate, would have chosen the particular combination of elements described in the claim. Instead, I have been informed that the correct analysis considers whether one of ordinary skill, facing the wide range of needs created by developments in the field of endeavor, would have seen a benefit to selecting the combination claimed.

42. I have been informed that, when determining whether a claimed invention is obvious, any “secondary considerations” of non-obviousness identified by the patentee should also be considered. These secondary considerations can include:

- commercial success of the invention, causally related to the invention itself rather than to companion factors, such as advertising or attractive packaging;
- the invention taught away from the technical direction followed by those skilled in the art;
- a long-felt but unsatisfied need for the invention while the needed implementing arts and elements had long been available;
- the invention achieves results unexpected to those skilled in the art;

- copying of the invention by competitors as distinguished from their independent development
- unsuccessful attempts by those skilled in the art to make the invention;
- acquiescence by the industry to the patent's validity by honoring the patent through taking licenses or not infringing the patent, or both; and
- skepticism, disbelief in or incredulity by those skilled in the art that the patentee's approach worked.

43. I have been informed that, for the above information to impact the obviousness of a patent claim, there must be a nexus between the alleged secondary considerations and the claims. In addition, I have been informed that the burden of introducing evidence of secondary considerations generally is on the Patent Owner. If the Patent Owner or its expert should assert secondary considerations of non-obviousness, I reserve the right to provide a Declaration addressing assertions of non-obviousness due to secondary considerations.

B. Claim Construction

44. I have been informed that claim terms are typically given their plain and ordinary meanings, as would have been understood by a person of ordinary skill

in the art at the time of the earliest alleged priority date. I have further been informed that when considering the meaning of any terms in the Challenged Claims of the '331 patent, I should apply the plain and ordinary meaning of those terms. I have further been informed that in considering the meaning of the claims, one must consider the language of the claims, the specification, and the prosecution history of record.

45. I have been informed that in general, a preamble limits the invention if it recites essential structure or steps, or if it is necessary to give life, meaning, and vitality to the claim. I have further been informed that a preamble is not limiting where a patentee defines a structurally complete invention in the claim body and uses the preamble only to state a purpose or intended use for the invention. I have further been informed that dependence on a particular disputed preamble phrase for antecedent basis may limit claim scope because it indicates a reliance on both the preamble and claim body to define the claimed invention. I have further been informed that clear reliance on the preamble during prosecution to distinguish the claimed invention from the prior art transforms the preamble into a claim limitation because such reliance indicates use of the preamble to define, in part, the claimed invention.

IV. PERSON OF ORDINARY SKILL IN THE ART AND THE TIME OF THE ALLEGED INVENTION

46. I have been asked to assume that the '331 patent is entitled to its earliest alleged priority date of September 24, 2010. *See* Ex. 1001. Beyond this

assumption, I have not undertaken an analysis to determine the earliest priority date to which the '331 patent is entitled.

47. Based on the materials and information I have reviewed and based on my experience in the technical areas relevant to the '331 patent, a person of ordinary skill in the art at the time of the alleged invention of the '331 patent would have had at least a Bachelor's degree in Computer Science or similar field and at least two years of industry experience in network security. More education can supplement practical experience and vice versa. Based on my knowledge and experience, including as discussed above in Section II, I was a person of ordinary skill in the art at the time of the alleged invention of the '331 patent and can provide opinions regarding the knowledge of a person of ordinary skill in the art as of that time. My opinions herein are, where appropriate, based on my understandings as to a person of ordinary skill in the art at that time. I myself had these capabilities at the time of the alleged invention of the '331 patent.

V. THE '331 patent

A. Technical Background

48. Below, I provide a brief background summary of the technology at issue.

49. U.S. Pat. No. 10,805,331 (the "'331 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.

50. For example, there were a number of well-known OSINT tools for collecting IP address information about assets. The McNab reference (Ex. 1005) 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.

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

52. 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.” McNab at 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.
```

53. Once the network hosts have been enumerated, they can then be scanned to assess information about the network. McNab itself explains that “Network

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.” McNab at 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.

54. 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” (Ex. 1015) 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

55. The paper then goes on to describe attacks such as the exploitation of vulnerabilities, or various forms of malware. Ex. 1015 at 9-14.

56. 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” (Ex. 1016), 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).” Ex. 1016 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.* at 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.* at 24.

Table 3-6. Risk-Level Matrix

Threat Likelihood	Impact		
			<i>High</i> (100)
<i>High</i> (1.0)	Low 10 X 1.0 = 10	Medium 50 X 1.0 = 50	High 100 X 1.0 = 100
<i>Medium</i> (0.5)	Low 10 X 0.5 = 5	Medium 50 X 0.5 = 25	Medium 100 X 0.5 = 50
<i>Low</i> (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

57. 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.” Ex. 1017 at 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.* at 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.* at 8. The chapter then explains how to use tools to perform “network discovery” using “DNS zone transfers, Whois requests, and reverse DNS lookups.” *Id.* at 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.*

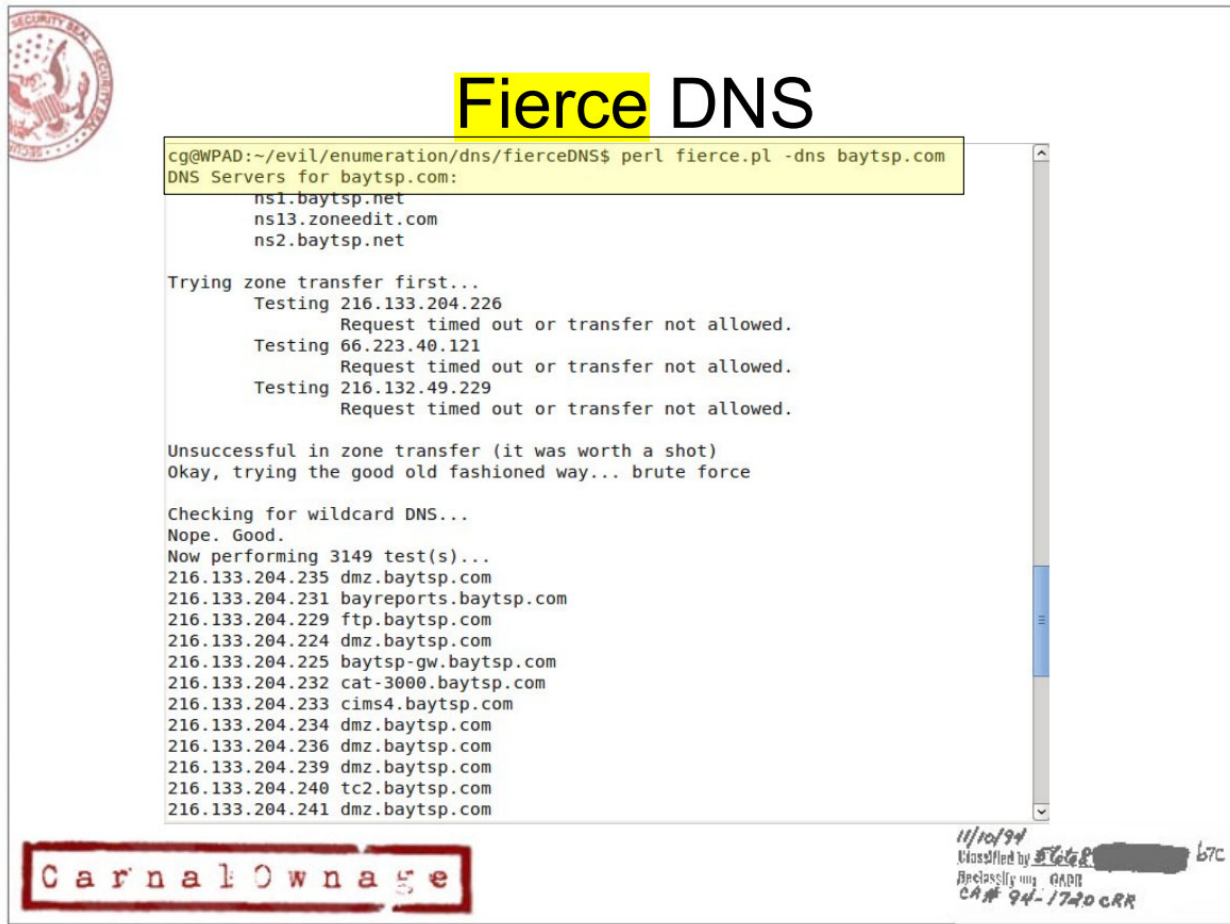
58. The paper also describes using “the Metasploit Framework” which “includes a number of application discovery modules ... to detect services that are difficult to find otherwise.” *Id.* at 14. For example, the below output searched on an IP range and returned DNS and SNMP services running on hosts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

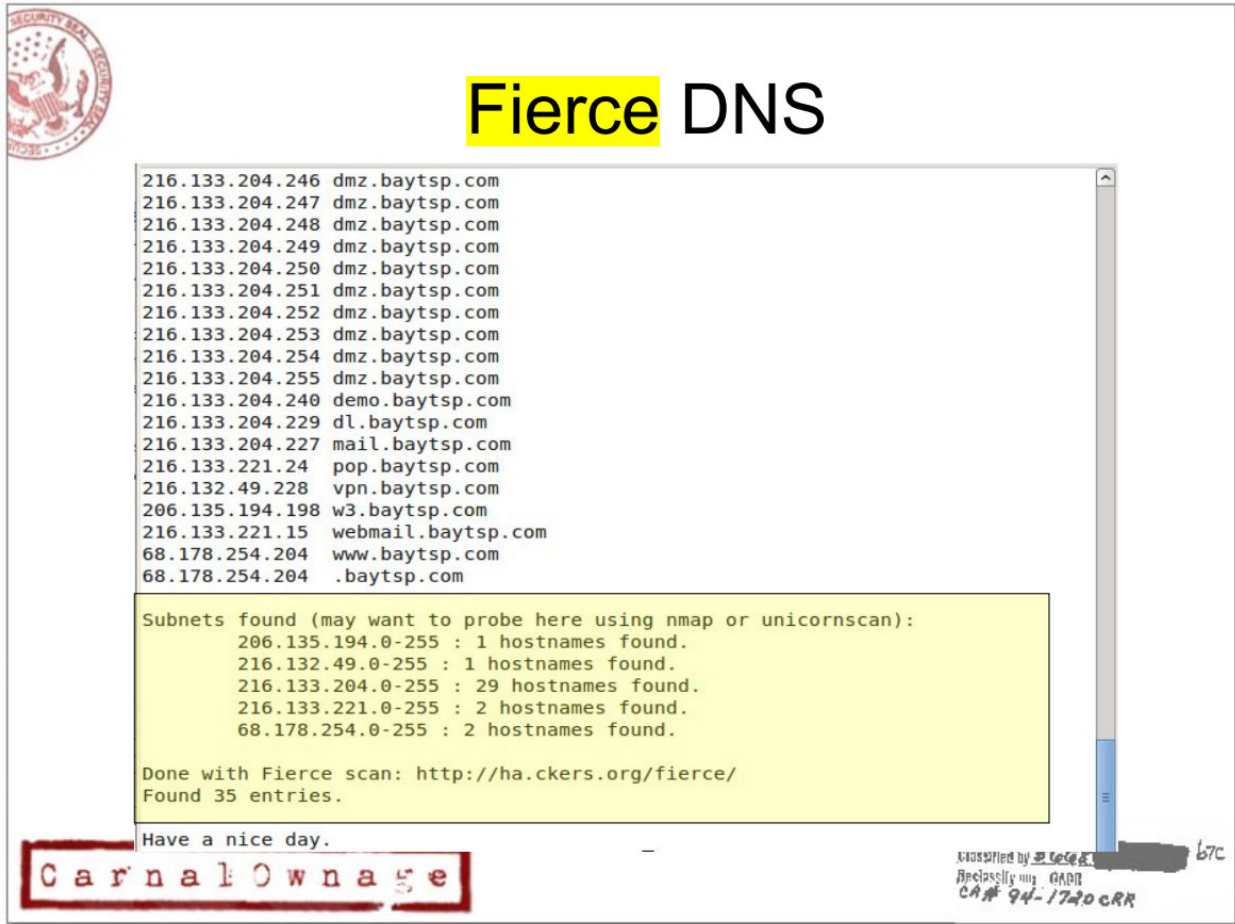
```
[*] Sending 6 probes to xxx.xxx.xxx.0->xxx.xxx.xxx.255 (256 hosts)
[*] Discovered DNS on xxx.xxx.xxx.19 (TinyDNS)
[*] Discovered DNS on xxx.xxx.xxx.249 (BIND 8.4.6-REL-NOESW)
[*] Discovered DNS on xxx.xxx.xxx.250 (Microsoft)
[*] Discovered SNMP on xxx.xxx.xxx.170 (Ethernet Routing Switch)
[*] Discovered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

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

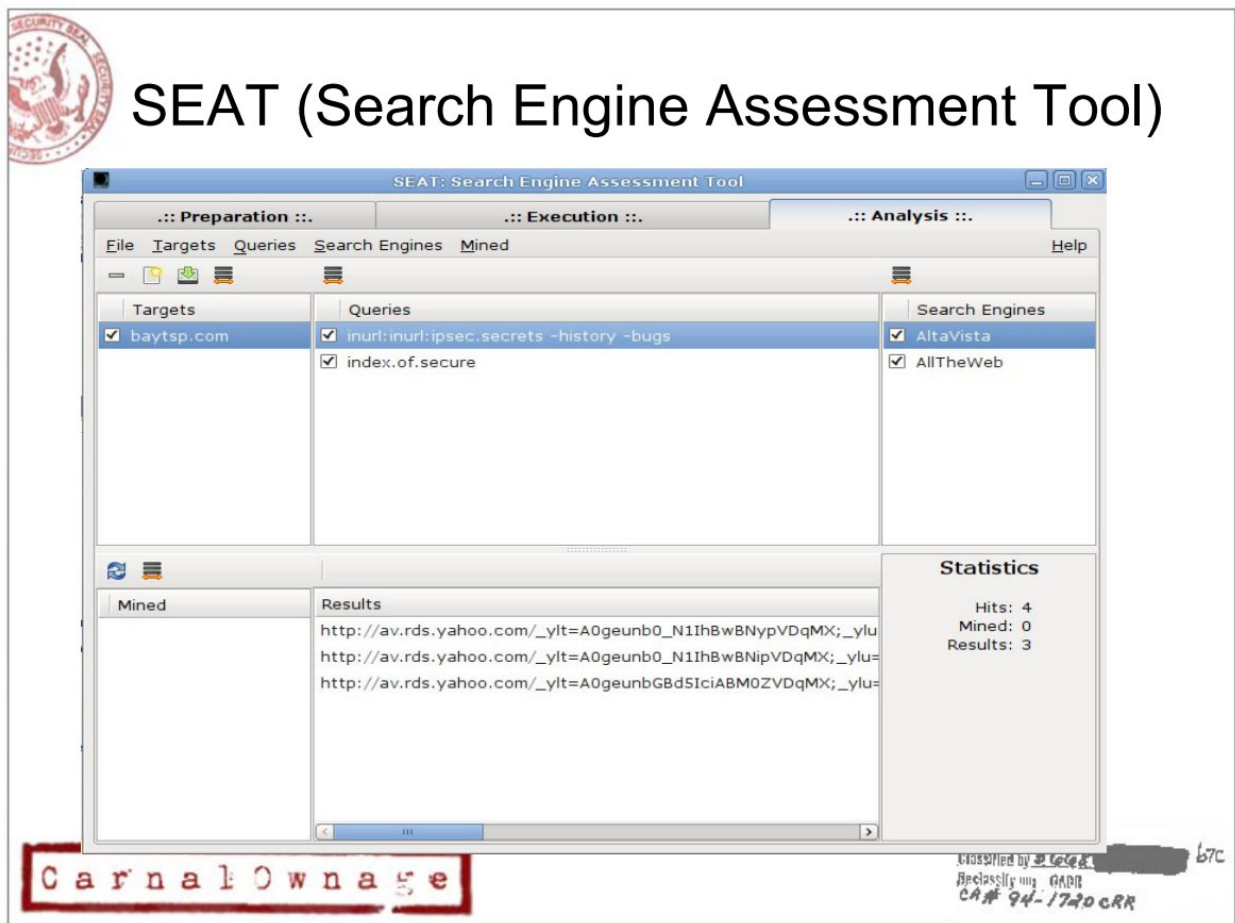
59. In 2008, a well-known security researcher named Chris Gates delivered a presentation called “New School Information Gathering” (Ex. 1018). The presentation describes a “[b]lack box approach to info gathering” where “the customer wants you to find everything about them you can via ‘open source’ methods.” Ex. 1018 at 5. OSINT information gathering involves “no direct contact with victim’s servers OR no non-standard traffic directed toward victim.” *Id.* at 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.* at 18. Fierce DNS uses a number of DNS queries to find hosts on the same domain and IP blocks used by the domain. *Id.* at 20. The below output for “baytsp.com” shows the various hosts for that domain name. *Id.* at 21-22.





60. 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.* at 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.* at 26.



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

62. 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.* at 35-40.

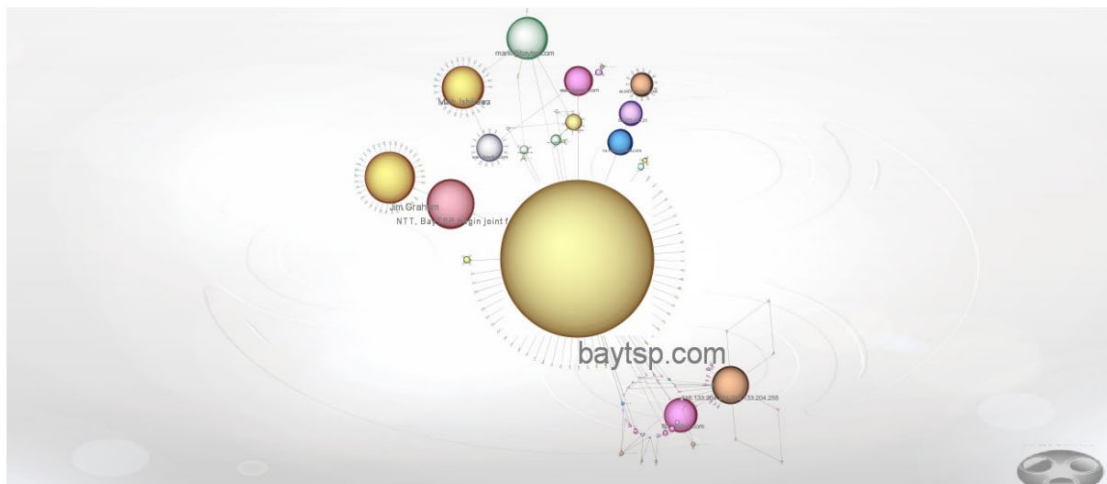
63. Finally, the presentation describes a tool called Maltego, which can perform many of the above functions automatically in one piece of software. Maltego

“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.* at 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.* at 67-72. From there, email addresses and documents can be harvested. *Id.* at 73-77. The presentation explains that Maltego can also search blogs, social networks and incoming links. *Id.* at 82. Maltego also provides graphical representations of the mapped network assets, showing them being associated with various entities. *Id.* at 80.



Maltego

- Sort your views to see relationships



Carnal O w n a g e

11/10/94
Classified by 57668 [redacted] 167C
Declassify on: OADR
CAF 94-1720 CRR

64. 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.

65. 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. Description of the '331 Patent's Specification

66. The '331 Patent to Boyer *et al.* was filed November 22, 2011 and claims priority to a provisional application filed September 24, 2010.

67. The '331 Patent is directed to conventional techniques for measuring the security vulnerability of a network from external observances. Specifically, it can “creat[e] a composite security rating” from data that is “derived from externally observable characteristics.” Ex. 1001 at Abstract. The claims of the '331 Patent further require that the composite score include metrics and data from information sources, some of which are on the Internet *See, e.g., id.*, cl. 1. These information sources provide information about an organization's network, its compromises and vulnerabilities, and resiliencies against such compromises and vulnerabilities.

C. The '331 Patent's Prosecution History

68. I have reviewed the prosecution history of the '331 patent and summarize it below.

69. During prosecution, the applicant's initial set of claims was significantly different than the claims that were eventually allowed. Ex. 1002, 898. 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.

70. Over several years, the applicant made gradual amendments to these claims, with each amendment rejected by the examiner, usually using the Newton reference (US 2004/0250122) in view of other references. *See, e.g.* Ex. 1002, 819-21, 755-757, 702-704, 665-667. On February 13, 2017, the examiner issued a final rejection on claims that largely resembled the allowed claims. *Id.*, 480-81, 435-454. The examiner found the claims unpatentable in view of Newton and Shull (US 2006/0212925). *Id.*

71. The applicant appealed the decision to the Board. On March 16, 2020, the Board reversed the obviousness rejection. *Id.*, 287-299. The Board agreed with the applicant that neither Shull nor Newton disclosed measuring “the resilience of the organization to recover from such vulnerability, the measure of the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability,” which was applicant’s only argument in their appeal brief. *Id.*, 291-94. While the examiner relied on Shull and Newton’s disclosure of reputational ratings, the Board found that they had nothing to do with “measuring *resilience*.” *Id.*, 293 (emphasis in original). The Board was also not convinced by the

examiner's argument that resilience is obvious in view of the reputational rating. *Id.*, 294.

72. However, the Board found that the claims lacked adequate written description for the notion of measuring resilience based on "the duration of the vulnerability." *Id.*, 295-97. Following the Board's order, the applicant removed that language from the claims. *Id.*, 276-77. The examiner then issued a notice of allowance. *Id.*, 37.

D. Interpretation of the '331 patent's Challenged Claims

73. For the purposes of my analysis in this IPR proceeding, I understand that the words of a claim are given their plain meaning that those words would have had to a POSITA at the time of the alleged invention. I also understand that the structure of the claims, the specification, and the prosecution history may also be used to better construe a claim insofar as the plain meaning of the claims cannot be understood. Moreover, I understand that even treaties and dictionaries may be used, albeit under limited circumstances, to determine the meaning attributed by a POSITA to a claim term at the time of filing. Furthermore, I understand that a Patent Owner's own apparent interpretation of certain terms in related proceedings can be considered to determine the meaning of patent claims in an IPR proceeding.

74. I have followed this approach in my analysis, and I have applied the plain and ordinary meaning of those terms as they would have been interpreted by a

POSITA at the time the invention was made (not today). For purposes of my analysis here, I have used the September 24, 2010 filing date of the '331 patent as the date of the invention.

VI. PUBLIC AVAILABILITY OF CERTAIN EXHIBITS

75. I have been asked to opine on the public availability of certain exhibits and specifically whether they were publicly available by September 24, 2010.

A. McNab

76. In my opinion, McNab was publicly available by 2008.

77. McNab is a book published by O'Reilly Media. I am familiar with O'Reilly Media and know that they are a very well-known and reputable publisher of books related to computer technology. I have reviewed dozens of O'Reilly-published books and have cited many such books in my own publications.

78. In my opinion, based on both my expertise in the field and from my personal experience, a POSITA would have considered O'Reilly Media to be a reputable publisher such that the copyright dates on their publications are a reliable and trustworthy indicator of when the publication was published. Ordinary artisans rely on the copyright date printed on the inside of O'Reilly-published books. I am not aware of nor have I heard of any O'Reilly-published book having a copyright date that is not commensurate with the date of its public availability.

79. In my opinion, Exhibit 1005 is also an authentic copy of McNab as it was available in 2008. Based on my significant experience as a reader of O'Reilly-published books, Exhibit 1005 is complete and has no visible alterations. Exhibit 1005 also has all the hallmarks of an authentic copy of an O'Reilly-published book, including a cover page, a copyright page, a table of contents, an index, and a back cover page. There are also no missing pages from Exhibit 1005. Thus, in my opinion, Exhibit 1005 is a true and authentic copy of McNab as it was published in 2008.

B. Internet Archive Pages

80. Several of the exhibits I have reviewed are from the Internet Archive, including Exhibits 1008, 1009, 1015, 1017, 1020, 1022, and 1023. I am familiar with the Internet Archive and have reviewed the declaration of Mr. Frank-White regarding the operation of the Internet Archive.

81. The Internet Archive exhibits are printouts of web pages or files that were archived by the Wayback Machine. Each link to the Wayback machine has a date and timestamp which indicates the date and time that the link was archived. In my experience this date and time an accurate reflection of when the Wayback Machine archives that particular page. Being familiar with the operation of the World Wide Web and crawlers like those used by the Wayback Machine, a page could not be archived by the Wayback Machine unless it was available to the public. Moreover, crawlers generally operate by accessing pages that were linked by other pages, and

therefore a page that was archived by the Wayback Machine is typically archived because it was linked from at least one other webpage. This further indicates that the archived webpage was publicly available at the time it was archived.

C. Public Videos

82. Exhibits 1019 and 1021 are printouts of webpages that host a video that was publicly available on Vimeo and YouTube, respectively.

83. Exhibit 1019 (available at <http://vimeo.com/2745624>) is a video on the Vimeo website entitled “Toorcon X Gates: New School Information.” This video is of Chris Gates presenting the presentation “New School Information Gathering,” a copy of which is at Exhibit 1018. The webpage states that it was uploaded on January 6, 2009. In my opinion, the upload date on a Vimeo webpage is generally a reliable indicator of when a video was publicly available. Ordinary artisans would have found the date on a Vimeo webpage to be a reliable indicator of public availability. I also note that Exhibit 1019 is a confirmation from an employee at Vimeo that the video was uploaded on January 6, 2009.

84. In addition, I note that Exhibit 1020 is the version of Exhibit 1019 as it was archived by the Wayback Machine on March 2, 2009. This indicates that the video was at least publicly available by March 2, 2009.

85. Thus, in my opinion, Exhibits 1018, 1019 and 1020 were all publicly available by early 2009. It is also my opinion that they are true and correct copies of

the video on the date they were published, since the video or webpage does not have any indication it was edited or altered since its upload date.

86. Exhibit 1021 (available at <https://www.youtube.com/watch?v=qiv4-wy3mxo>), is a video on the YouTube website entitled “Social Engineering Using Maltego.” Exhibit 1031 are screenshots of relevant portions from this video. The webpage states it was uploaded on September 14, 2009 and that it has thousands of views. In my opinion, the upload date on a YouTube webpage and its view count is generally a reliable indicator of when a video was publicly available. Ordinary artisans would have found the date on a YouTube webpage to be a reliable indicator of public availability. Moreover, the metadata for this video indicates that it was “published[]At” September 14, 2009 and has a “view[]Count” of 60,168 views, thereby further indicating its public availability by 2009. Ex. 1030.

87. I also note that the video itself, which is of a person using the Maltego software, often displays various dates. All of these dates are consistent with a public availability date of 2009. For example, at 0:20, the video shows an NS record that is dated March 23, 2009.

88. This in my opinion, Exhibit 1021 was publicly available by 2009. It is also my opinion that they are true and correct copies of the video on the date they were published, since the video or webpage does not have any indication it was edited or altered since its upload date.

VII. GROUND 1: TIPPETT, MCNAB AND MCGOVERN RENDER OBVIOUS CLAIMS 1-29

89. Tippetts discloses systems and methods for collecting information from a number of external sources, both public and private, about an entity's information resources in order to generate a composite rating in the form of a security risk index. The collected information includes information about past incidents of security breaches, security events that may be unique to the entity, and mitigation measures. Tippetts further discloses providing reports about an entity's security risk index to the entity's business partners to make business decisions based on the measured risk.

90. McNab discloses a number of methodologies for remotely collecting information about the security of entities, such as performing a vulnerability scan that determines whether security breaches have occurred or whether a mitigating antivirus software has been installed. It would have been obvious to incorporate these teachings into Tippetts as one of the sources of information.

91. Finally, McGovern discloses collecting information about the duration of security breaches as well as presenting security assessments using a web portal, which also would have been obvious to incorporate into Tippetts as one of the sources of information.

A. Rationale to Combine

92. In my opinion, a POSITA would have found it obvious to combine Tippetts's methods for collecting information from various sources to generate security

risk indices with McNab's teachings of collecting security and IP address information about network assets and McGovern's teachings of determining the duration of a malicious activity as well as its teachings of assessment scores in a web-based user interface.

1. McNab

93. In my opinion, a POSITA would be motivated to incorporate McNab's teachings of enumerating assets by collecting their IP addresses as well as its teachings of using a vulnerability scanner to collect security information about those assets. Such teachings were known to provide useful and necessary information to assess the security risk of an organization's network.

94. McNab is an O'Reilly-published book entitled "Network Security Assessment" and describes various tools and methodologies for assessing the security of a network. McNab at Cover. In particular, McNab discloses a "Network Security Assessment Methodology" that begins with "Internet Host and Network Enumeration" to identify IP addresses of network assets, and then performing "Bulk Network Scanning and Probing" and "Investigation of Vulnerabilities." McNab at 4-7. For example, McNab discloses methods such as "DNS Querying" and a "zone transfer" to obtain IP addresses of computer within a domain. McNab at 30-35. And for vulnerability scanning, McNab discloses the use of a tool called Nessus that "can be used to perform a number of network-wide bulk security checks." McNab at 377.

McNab discloses that Nessus includes a number of plug-ins that were available on the Nessus website. McNab at 377, 390; Exs. 1008, 1009, 1023.

95. A POSITA would have been motivated to incorporate these teachings from McNab to provide a well-known and reliable method of determining the IP addresses of assets and performing well-known vulnerability scans on those assets. Tippet already describes generating “a security risk index for assessing the security of information resources,” which includes an entity’s “databases,” “computer terminals,” or “servers.” Tippet at ¶32. Tippet also describes generating the security risk index by using “information relating to the security of information resources.” Tippet at ¶33. A POSITA would have been motivated to give effect to these teachings in Tippet by using the techniques disclosed in McNab to identify the information resources (such as by their IP address) and to perform vulnerability scans to collect security information about those information resources. In addition, as discussed above in the background, the use of these tools to enumerate network assets (including enumerating their IP addresses) using public information sources was well-known and could be accomplished using automated tools such as Maltego (which itself uses well-known DNS queries). Network enumeration and security risk assessment were also well-known and ubiquitous methods for helping secure an organization’s networks. A POSITA would be motivated in view of this knowledge to automatically gather information from information sources as disclosed in Tippet by using tools described

in McNab and generally known to a POSITA, such as DNS query tools like Maltego. As discussed above, such tools also provided security risk assessment scores, providing additional motivation to combine Tippet and McNab.

96. In addition, a POSITA would have been motivated to use McNab's teachings because of the well-known benefits of determining IP addresses of network assets to perform vulnerability scans on those assets. McNab itself teaches the importance of its methodologies: "[t]o retain complete control over your networks and data," and to "take a proactive approach to security ... that starts with assessment to identify and categorize your risks." McNab at 1. McNab also emphasizes the "Business Benefits" of network security assessment, which is "a business enabler." *Id.* McNab also explains that the book describes "assessment of technical security and ***improving the integrity and resilience of IP networks.***" *Id.* at 2.

97. With respect to McNab's teachings of determining IP addresses of network assets, a POSITA would have been motivated by McNab's teaching explains that they provide "useful data about the structure of the target network" and that such "[i]nitial reconnaissance is very important because it can uncover hosts that aren't properly fortified against attack." *Id.* at 5. As McNab points out, companies "often neglect hosts and networks that lay off the beaten track," giving attackers access to "peripheral networks and hosts" that were not prioritized. *Id.*

98. Finally, with respect to using the Nessus vulnerability scanner, a POSITA would have been motivated by McNab's teaching that it "significantly reduc[es] the amount of time spent during a penetration test performing manual checks." *Id.* at 377. A POSITA would have also been motivated by its capabilities to scan for specific malware such as MS Blaster worm or W32.SoBig, since it would be highly beneficial to know which assets have been breached in order to mitigate and recover to return the network to a secure status.

99. In addition, it would have been obvious to incorporate the teachings with respect to Nessus that are described in Exhibits 1008-1009 and 1023. Exhibits 1008-1009 and 1023 are archived webpages that provide additional detail about the Nessus product described in McNab. Thus, a POSITA would be motivated to include such additional functionality, such as the plug-ins which detect malicious software such as MSBlaster and So.Big (Exs. 1008-1009), or the plug-in which detects the presence of Symantec Anti Virus software (Ex. 1023), because they describe improved security capabilities and displays. A POSITA would have a reasonable expectation of success because these documents describe the Nessus product and therefore do not require any modifications to the product itself.

100. Thus, given all of the above motivations as known by a POSITA and as taught in McNab, a POSITA would have been motivated to combine Tippet and McNab to improve the security and resilience of the network.

101. A POSITA would have reasonably expected success in combining Tippet with McNab's teachings. McNab provides detailed and sufficient information to perform asset enumeration (such as using DNS querying and requesting a zone transfer) and vulnerability scanning (such as using Nessus). It would have been well within the capabilities of a POSITA to incorporate such mechanisms, especially since Tippet discloses "information sources" that include "sensors" to which a POSITA could incorporate McNab's teachings.

102. Finally, Tippet and McNab are directed to the same field endeavor as the '331 patent, the field of network security. Tippet 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. The security risk index may represent the security of information resources."); McNab at xvi ("This book tackles one single area of information security in detail: that of undertaking IP-based network security assessment in a structured and logical way."); Ex. 1001 at Abstract ("A method and system for creating a composite security rating from security characterization data of a third party computer system.").

2. McGovern

103. In my opinion, a POSITA would be motivated to incorporate McGovern's teachings of calculating a duration of malicious activity as well as a remote web-based user interface because such teachings were known to increase the

security of a network as well as increase user-friendliness of the system and provide the user an easier assessment of the network, including by remotely accessing such assessments. Simplifying the display of security information would be of paramount interest to a POSITA as it would aid in identifying and addressing security breaches and other security issues within the user's network.

104. McGovern discloses the capability of determining the “average response or patch time after security breach detection.” McGovern at ¶38. A POSITA would be motivated to incorporate this teaching into Tippet, which discloses gathering information about security breaches of an entity's network to generate a security risk index, because of the known benefits. As an initial matter, Tippet discloses calculating “effectiveness of the specific implemented mitigating measure” of an entity's network, which includes “various aspects of mitigation” such as “a detection aspect” and “a recovery aspect.” Tippet at ¶52. A POSITA would be motivated to give effect to this teaching by incorporating McGovern's teaching of calculating a “response or patch time after security breach detection,” which would make use of Tippet's “detection aspect” and “recovery aspect” of the mitigating measure.

105. In addition, a POSITA would understand that it would be beneficial to include the duration of a security breach in the security risk index of Tippet, because the duration of a security breach is an important factor in determining overall network security. A POSITA would understand that a security breach is an incredibly

dangerous event that puts all of the organization's data and resources at risk of damage or theft. A POSITA would further understand that a security breach can cause damage to the company via various ways, including the theft of confidential information, putting the business at a competitive disadvantage, or the theft of customer or employee information, therefore harming said customers or employees, harming the company's reputation, and increasing the liability risk to the company. A POSITA would therefore understand that it would be highly desirable to minimize the duration of any security breach—thus, it would be beneficial for a network administrator to know whether the network and the organization's IT policies are robust and proactive to such security breaches (resulting in a minimal duration) or if they are particularly vulnerable (because of a lengthy duration).

106. McGovern also discloses the capability of displaying a network assessment score in “a software program with a user interface,” which can be “designed to run as a Web-based service or application” wherein users can “access the scoring and related functionalities remotely via standard browsers or similar user interfaces.” McGovern at ¶¶42, 45. A POSITA would be motivated to incorporate these teachings into Tippet because it allows network administrators access Tippet's reporting function from anywhere an Internet browser is available—at the time of the '524 patent, that would have included smartphones. A POSITA would therefore be

motivated to make this combination in order to increase ease-of-use and accessibility, as well as responsiveness to security events.

107. A POSITA would have combined Tippet and McGovern with a reasonable expectation of success. Tippet is directed to collecting information about mitigating measures and security events for an entity in order to generate a security risk index. Adding McGovern's teaching of determining the duration of a security breach would be piece of information that an administrator could perform that was well-within the capability of a POSITA at the time of the '524 patent, especially in view of Tippet's teachings of using a "detection aspect" and "recovery aspect" of a mitigating measure. Tippet at ¶52.

108. A POSITA would have also reasonably expected success in combining Tippet with McGovern's remote user interface. This would involve presenting the security risk indices as taught in Tippet using McGovern's web portal and would have been well-within the capabilities of a POSITA at the time of the '524 patent.

109. Finally, Tippet and McGovern are analogous to the '331 patent because all are directed to the same field of endeavor, the field of network security. Tippet 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. The security risk index may represent the security of information resources."); McGovern at Abstract ("Methods for information security assessment and data risk scoring are

disclosed.”); Ex. 1001 at Abstract (“A method and system for creating a composite security rating from security characterization data of a third party computer system.”).

B. Claim 1

1. **1[pre], 1[a]: A method comprising: collecting information about two or more organizations that have computer systems, network resources, and employees, the organizations posing risks through business relationships of the organizations with other parties,**

110. With respect to the limitation “*A method comprising: collecting information about two or more organizations that have computer systems, network resources, and employees,*” Tippet discloses a method for performing security assessments by collecting information of various entities including corporations. Specifically, Tippet discloses a method for determining a “security risk index,” which is an assessment of “the security of information resources” that uses *information* such as “frequency of security events,” “likelihood of a security event breaching the security of the information resources,” and “expected cost of a breach of the security of the information resources.” Tippet at ¶23.

111. The security risk index is generated for one or more “entities 224.” *Id.* at ¶31 (“security risk index determining unit 212 may be operatively coupled to at least one of a plurality of entities 224”), ¶46 (“[A] local security risk index may ... be determined for any other entity or group of entities.”); Fig. 4B. An “entity” “may include an individual; a group of individuals; an institution; a community; an

organization; a group of institutions within an industry; a group of institutions of the same approximate size; a group of individuals, institutions, or other organizations within a country; or any other entity,” as well as “consultants, vendors, customers, home users.” *Id.* at ¶32. Thus, a POSITA would understand that an “entity” includes ***organizations that have employees***, such as a company within an industry. An entity further has “databases,” “computer terminals,” “computer networks,” “servers,” and “other information resources,” *i.e. computer systems and network resources. Id.*

112. With respect to the limitation ***“the organizations posing risks through business relationships of the organizations with other parties,”*** Tippet discloses that the entities (*i.e. organizations*) have ***business relationships with other parties*** and that the security assessments of those entities reflect ***risks posed by the entities to those parties.***

113. Specifically, Tippet discloses that the “security risk index” is used to “certify the security” of an entity, and that certification may be given to “outside parties such as clients, partners, insurers, vendors, consultants, associates, competitors, or other parties,” *i.e. parties with business relationships with the organizations.* Tippet at ¶62. The certification “verif[ies]” to those parties that the entity’s resources are “secure.” *Id.* Thus, a POSITA would understand that Tippet discloses a method for certifying to third parties that the entity does not ***pose a security risk to those business partners.*** A POSITA would therefore understand that if the entity’s security risk index

does not meet the certification threshold, the resources of the entity may *pose a risk* to the business partners. It was, for example, well-known that assuring the security of information, “[f]rom a commercial standpoint, ... is a *business enabler*.” McNab at 1 (emphasis in original).

2. **1[b]: the information collected about the organizations being indicative of compromises, vulnerabilities or configurations of technology systems of the organizations and indicative of resiliencies of the organizations to recover from such compromises, vulnerabilities or configurations,**

114. With respect to the limitation “*the information collected about the organizations being indicative of compromises, vulnerabilities or configurations of technology systems of the organizations,*” Tippet discloses that the “security risk index” is evaluated using information *indicative of the entity’s compromises, vulnerabilities or configurations*. Specifically, Tippet discloses generating a “local security risk index 410 for the entity,” and that such indices can be generated for multiple entities. Tippet at ¶¶48, 46. The security risk index incorporates information related to “a past history of at least one type of security breach,” *i.e. information about the organization indicative of compromises*. *Id.* at ¶49. The security risk index also incorporates information related to “the local vulnerability of the information resources associated with the entity” or “a type of possible security breach that is unique to ... the entity,” *i.e. information about the organization indicative of vulnerabilities*. *Id.* at ¶¶48-49. Finally, the security risk index incorporates information related to “a rate

or frequency at which a specific type of security event [was] experienced by the entity.” *Id.* at ¶50. Such “security events” include “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,” and therefore is **information about the organization indicative of configurations**. *Id.* at ¶37. Security events also include “attack from hackers,” and is therefore also information **indicative of compromises** as well as **vulnerabilities**, since a POSITA would understand that many if not most hacker attacks involve exploitation of vulnerabilities. *Id.* at ¶3.

115. With respect to the limitation **“and indicative of resiliencies of the organizations to recover from such compromises, vulnerabilities or configurations,”** Tippettt also discloses that the security risk index incorporates information about **resiliencies to recover from compromises, vulnerabilities or configurations**. Specifically, Tippettt discloses that the security risk index incorporates information related to “certain mitigating measures designed to secure information resources that is unique to ... the entity,” “a future plan for securing the information resources associated with the entity,” “effectiveness of a mitigating measure designed to secure information resources that has been employed by the entity,” “effectiveness of a specific implemented mitigating measure to safeguard information resources against a specific type of security event,” “a past rate of success for a specific type of security

event against the entity,” and “mitigating measures [that] will prevent the specific type of security event from causing a breach of security.” *Id.* at ¶¶49-51, 53. All of these are information that is *indicative of resiliencies of the organization to recover from* security events, security breaches and other vulnerabilities (*i.e. compromises, vulnerabilities or configurations*).

116. McNab also discloses collecting *information indicative of compromises or vulnerabilities of an organization or resiliencies to such compromises or vulnerabilities*. In particular, McNab discloses various methods for collecting the information described by Tippet, such as information related to the “vulnerability of the information resources with the entity” or “mitigating measures [that] will prevent the specific type of security event from causing a breach of security.” Tippet at ¶¶50, 53. Although Tippet does not explain in detail the methodologies for collecting the above information, as discussed above, a POSITA would have combined Tippet with McNab’s teachings to obtain the above information about compromises and vulnerabilities.

117. For example, McNab discloses a vulnerability scanning tool called Nessus that “can be used to perform a number of network-wide bulk security checks.” McNab at 377. These scans are performed by a server that installed the Nessus server software. *Id.* These checks are “remote network-based security checks, testing how the target host responds to specific network probes.” *Id.* McNab further discloses that

Nessus can perform a number of vulnerability scans depending on the “plug-in[s]” that are installed on the Nessus server. *Id.*; Fig. 15-3. These plug-ins are described on Nessus’s website. *Id.* at 390.

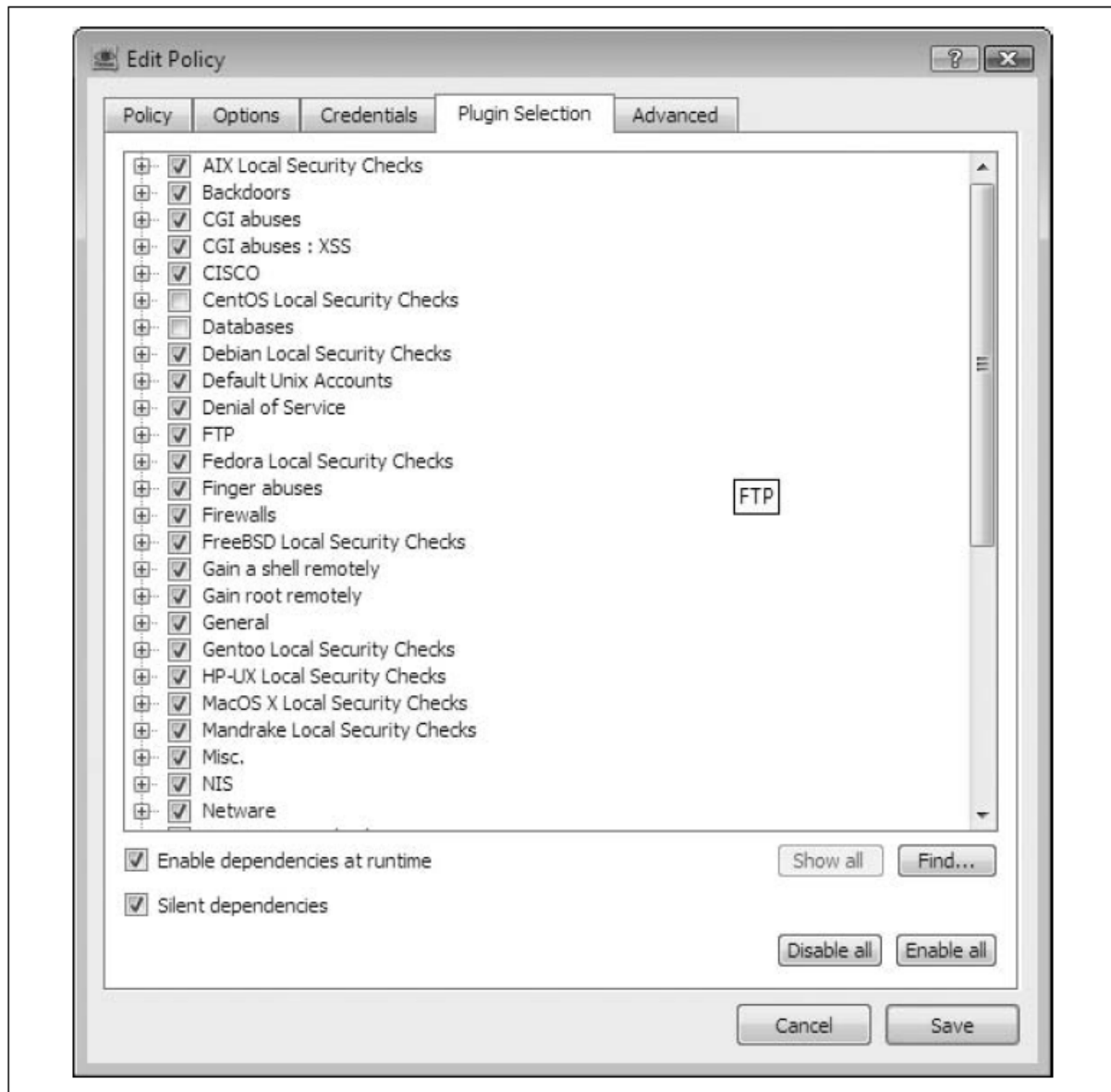


Figure 15-3. NessusClient 3 plug-in selection window

118. For example, one of the Nessus plug-ins includes detecting whether “[t]he remote host [is] infected by the MS Blaster worm.” Ex. 1008. Another plug-in

detects the presence of a number of viruses, such as variants of the W32.SoBig worm. Ex. 1009. These vulnerability scans are information related to the “vulnerability of the information resources with the entity,” *i.e. information indicative of compromises or vulnerabilities of an organization*. Tippet at ¶50. Another Nessus plug-in “checks that the remote host has Symantec AntiVirus Corporate installed and properly running, and makes sure that the latest Vdefs are loaded.” Ex. 1023. This scan is information related to “mitigating measures [that] will prevent the specific type of security event from causing a breach of security,” *i.e. information indicative of resiliencies to compromises or vulnerabilities*. Tippet at ¶53. The results of the scans are described in reports which can be exported to a number of formats. McNab at ¶¶390-91.

3. 1[c]: the information indicative of durations of events associated with compromises or vulnerabilities or configurations,

119. Tippet discloses that the security risk index incorporates information related to “an *effectiveness* of a mitigating measure designed to secure information resources that has been employed by the entity.” *Id.* at ¶50. A POSITA would understand that the “effectiveness of a mitigating measure” includes the *duration of events associated with compromises or vulnerabilities or configurations*, such as the duration of a security breach or vulnerability before the mitigating measure mitigates the event, because effectiveness cannot be properly measured without also considering how long the network remained vulnerable or compromised. This is also supported by

Tippett’s disclosure that the mitigating measure includes both “a *detection aspect*” and “a *recovery aspect*,” which together would indicate the duration of the malicious event. *Id.* at ¶52.

120. A POSITA would also consider it obvious that the effectiveness of a mitigating measure would include the duration it took to mitigate the malicious event. A POSITA would have been motivated to include the duration of the event because the duration a network is compromised or vulnerable is directly correlated with many undesirable factors, such as (1) the number of assets that have been compromised, (2) the amount and/or value of information that may have been misappropriated, (3) the cost and time to fully remove the malicious software, and (4) the legal liability and negative public reaction to the attack. A POSITA would desire to minimize all of these, and therefore minimize the duration of the compromising event. Thus, a POSITA would find it desirable to measure the effectiveness of a mitigating measure by including the duration it takes to fully mitigate a security event, and not merely the fact that the security event was mitigated. A POSITA would have had a reasonable expectation of success because it was well within the skill of a POSITA to measure the time between detection of the malicious event and recovery from the malicious event, both of which Tippett discloses are part of the “mitigating measure.” Tippett at ¶52 (“An aspect of mitigation may include ... a detection aspect [and] a recovery aspect”).

121. In addition, McGovern teaches measuring a security parameter such as “average response or patch time after security breach detection.” McGovern at ¶38. A POSITA would understand this teaching to be information *indicative of durations of events associated with compromises or vulnerabilities or configurations*. As discussed above, a POSITA would have considered it obvious to combine Tippet and McGovern.

4. 1[d]: at least some of the information about each of the organizations being collected automatically by computer using sensors on the Internet,

122. Tippet discloses that the determination of the security risk index is performed by a “security risk index determining unit 212” which is connected to “a plurality of *information* sources 242 ... via the network 228.” Tippet at ¶33. Tippet further discloses that the information sources includes “*sensors*.” *Id.* The “network 228” includes the *Internet*, and thus the information sources are *sensors on the Internet*. *Id.* at ¶34 (“Examples of one or more networks may include ... the Internet”). In addition, a POSITA would understand that the information sources listed by Tippet indicate are typically Internet sources, such as “network chat forums,” “network message boards,” “scholarly journals,” “periodicals,” and “commercial web pages.” *Id.* at ¶33.

123. A POSITA would understand that such information was *collected automatically* because such information includes information about “security events

that lead to breaches in security, a number of security events that do not lead to breaches in security, a probability that a certain type of security event will lead to a breach in security, a prevalence of certain mitigating measures designed to secure information resources, or any other suitable type of information.” *Id.* at ¶40. A POSITA would understand that such information, if collected by “sensors,” would be collected automatically.

124. A POSITA would understand that the information disclosed in limitations 1[a] through 1[c] used for generating the security risk index is collected by the “information sources 242.” Tippet discloses that the process for calculating the “general security risk index” involves “determination of the general vulnerability factor 306” which gathers “information relating to a likelihood of a security event breaching the security of information resources on the network 228.” Tippet at ¶40. Such information is located at “at least one information source 242.” *Id.* A POSITA would therefore understand that for calculating the “local security risk index” for the “entity,” it would likewise use the information sources. This is because, as with the general security risk index, the “local security risk index” uses a “local vulnerability factor” which requires similar types of information as used for the “general vulnerability factor,” but directed to an “entity 224” instead of the general “network 228.” *Id.* at ¶¶48-51. Moreover, Tippet does not otherwise specify the information sources for the “local vulnerability factor” and thus a POSITA would understand that

they would be the “information sources 242” that are coupled to the “security risk index determining unit 212” (which is itself coupled to the plurality of entities 224). *Id.* at ¶¶31, 33.

125. A POSITA would have also considered it obvious that the information for calculating the “local security risk index” comes from the “information sources 242.” A POSITA would be motivated to do this in order to give effect to Tippet’s teachings wherein the “local vulnerability factor” makes use of several pieces of information, including the information discussed in limitations 1[a] through 1[c], because Tippet does not otherwise explain the source of such information. A POSITA would be motivated by Tippet’s teachings that the “global vulnerability factor” collects similar information from the “information sources,” and thus the “local vulnerability factor” should likewise collect information from the “information sources.” A POSITA would also be motivated by the fact that the “information sources” includes “sensors,” “machine records,” “public databases” and “trust values,” all of which were known to collect the types of information used by the “local vulnerability factor. A POSITA would have had a reasonable expectation of success in having the security risk index determination unit simply use the information sources to gather the information used for the “local vulnerability factor.”

126. In addition, McNab discloses that the Nessus vulnerability scanning, which would have been obvious to combine with Tippet, *automatically collects*

information via sensors on the Internet. McNab discloses that Nessus performs “[v]ulnerability scanning us[ing] **automated** systems ... with minimal hands-on qualification and assessment of vulnerabilities,” and that it “significantly [reduces] the amount of time spent during a penetration test performing manual checks.” McNab at 3, 377. McNab also discloses that Nessus can be “start[ed]” automatically “by using an operating system-appropriate startup file.” *Id.* at 382. Finally, McNab also discloses a “command-line client for scanning,” and POSITA would have understood that a command line can be automated by using any number of well-known techniques, such as the “cron” command in UNIX or “Task Scheduler” in Windows. A POSITA would have considered it obvious to use the “cron” or “Task Scheduler” utility to automate performing scans using Nessus, as that would provide the well-known benefit of allowing for regularly scheduled vulnerability scans to ensure network assets are not vulnerable. A POSITA would have had a reasonable expectation of success because “cron” and “Task Scheduler” were utilities a POSITA would have been familiar with.

127. McNab also discloses gathering information via *sensors on the Internet*. McNab discloses that Nessus is “a free **vulnerability scanner** that can be used to perform **a number of network-wide** [*i.e. multiple sensors*] bulk security check.” *Id.* at 377. The Nessus client “configures the various target, scanning, and plug-in options, and it reports the findings from the scan to the user.” *Id.* These configurations and plug-ins are each a **sensor**. McNab further discloses that Nessus

performs its scans using a server on *the Internet*. Specifically, the “Nessus server performs all of the scanning and security checks” and is “Internet-connected.” *Id.* at 377, 383.

5. **1[e]: the information about each of the organizations being collected from two or more sources, one or more of the sources not being controlled by the organization, the information from at least the one or more sources that are not controlled by the organization being collected without permission of the organization,**

128. With respect to the limitation “*the information about each of the organizations being collected from two or more sources, one or more of the sources not being controlled by the organization,*” Tippet discloses multiple information sources, several of which are not *controlled by the organization*. Specifically, Tippet discloses that there are “a plurality of information sources,” *i.e. two or more sources*. Tippet at ¶33. Tippet further discloses that the information sources include “public databases, network chat forums, network message boards, scholarly journals, periodicals, personal and commercial web pages.” *Id.* A POSITA would understand that not all of these sources of information would be controlled by the target organization, because at the time of the patent, there was no single organization that simultaneously controlled chat forums, message boards, scholarly journals, periodicals, and personal and commercial web pages. A POSITA would understand that the vast majority of organizations would not control any of such types of information sources. Instead, a POSITA would understand that such sources were

controlled by the persons or companies that owned such web pages, which typically would not be the organization for which information is being collected.

129. McNab also discloses that the Nessus vulnerability scan, which would have been obvious to combine with Tippet, collects information without control from the organization. As a general matter, McNab discloses that “the methodology presented in this book describes how a determined *attacker* will scour Internet-based networks in search of vulnerable components.” McNab at xvi. The purpose of the book is to teach network administrators to “assess[] your networks in the same way that a determined attacker does.” *Id.* In other words, the methodologies in McNab, including the Nessus vulnerability scanner, were performed without control from the organization. With respect to Nessus specifically, McNab discloses that it will “run without credentials” which “test[s] how the target host responds to specific network probes.” *Id.* at 377. In addition, Nessus performs its vulnerability scanning by simply specifying “[t]he target network addresses or hosts to be scanned,” which would be any address or host that was not affiliated with the Nessus user. *Id.* at 384. Such tests and scans are performed outside of the organization’s network, and can be performed remotely by anyone using Nessus. *Id.* at 377 (“Nessus will perform remote network-based security checks, testing how the target host responds to specific network probes.”). Thus, McNab discloses collecting information *without being controlled by the organization*.

130. With respect to the limitation “*the information from at least the one or more sources that are not controlled by the organization being collected without permission of the organization,*” Tippet discloses that one or more of the information sources is *collected without permission of the organization*. Tippet discloses that the information sources include “network chat forums, network message boards, scholarly journals, periodicals, personal and commercial web pages.” Tippet at ¶33. In addition, Tippet discloses that some of the information is directed to general information of interest to any security researcher, like “security events that lead to breaches in security,” “effectiveness of a mitigating measure,” or “a past rate of success for a specific type of security event.” *Id.* at ¶¶40, 50. 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 the information was *collected without permission of the organization*. A well-known example at the time of the patent would be databases that describe various vulnerabilities, exploits, and malware that could target any organization (such as MITRE)—such information would have been compiled by security researchers not affiliated with an organization and thus collected without permission from the organization. For example, information about malware like MSBLASTER would have been collected without permission from any particular organization. Moreover, since the network scanning tools described in McNab can be performed by any Internet user

(such as DNS queries), a POSITA would expect such information to be collected and stored in the information sources without permission from the organization.

131. Similarly, as discussed above, McNab discloses that its methodologies assess “networks in the same way that a determined attacker does,” *i.e. without permission from the organization*. McNab at xvi. And Nessus can target any network address or hostname to perform its vulnerability scan, including those *without permission from the organization*. McNab at 377, 384.

6. 1[f]: at least partly automatically gathering information about assets that each of the organizations owns, controls, uses, or is affiliated with, including IP addresses and IP network address ranges, computer services residing within address ranges, or domain names,

132. With respect to the limitation “*at least partly automatically gathering information about assets that each of the organizations owns, controls, uses, or is affiliated with,*” Tippet discloses automatically gathering information about information resources, *i.e. assets of an organization*. First, Tippet describes “information resources” as “data, networks, systems, information, business intelligence, hardware, software, and other resources,” *i.e. assets*. Tippet at ¶2. Tippet discloses that “entity 224A [*i.e. an organization*] may be associated with various information resources.” Tippet at ¶32. And as discussed above for limitations 1[a] through 1[c], Tippet discloses *automatically gathering information about*

information resources, such as information about security breaches, vulnerabilities, and mitigating measures. Tippet at ¶¶48-51.

133. With respect to the limitation “*including IP addresses and IP network address ranges, computer services residing within address ranges, or domain names*,” Tippet does not explicitly disclose gathering IP addresses, address ranges, or domain names for the information resources. However, McNab discloses several methods for gathering IP addresses of information resources, and as discussed above, it would have been obvious to combine Tippet and McNab.

134. In particular, McNab dedicates an entire chapter to “Internet Host and Network Enumeration” which describes gathering information such as “internal IP addresses” and “the target organization’s DNS structure (including domain names, subdomains, and hostnames).” McNab at 5; *see* Chapter 3 (“Internet Host and Network Enumeration”). One method is to use “DNS Querying,” which retrieves information about “Hostnames” and in some cases, enumeration of “Names and IP addresses of internal or nonpublic hosts.” McNab at 30. McNab gives an example of using the domain “cia.gov” to discover several other assets and their IP addresses within the cia.gov or ucia.gov domain. *Id.* at 30-31. Another “popular method for gathering information about *all the computers within a DNS domain*” involves requesting “a zone transfer,” which returns a “DNS zone file contain[ing] all the naming information

that the name server stores regarding a specific DNS domain,” including *hostnames, IP addresses, and IP address blocks*. *Id.* at 32-35.

7. 1[g]: at least one of the sources for each of the organizations comprising a public source or a commercial source,

135. Tippetts discloses that several of the information sources that collect the information discussed in limitations 1[a] through 1[c] include “*public* databases, network chat forums, network message boards, scholarly journals, periodicals, personal and *commercial* web pages” and “*public* databases created by data mining any or all of the aforementioned information sources.” Tippetts at ¶33.

8. 1[h]: processing by computer the information from the two or more sources for each of the organizations to form a composite rating of the organization that is indicative of a degree of risk to the organization or to a party through a business relationship with the organization, the composite rating comprising a calculated composite of metrics and data derived or collected from the sources,

136. With respect the limitation “*processing by computer the information from the two or more sources for each of the organizations to form a composite rating of the organization,*” Tippetts discloses the calculation of a “local security index” for an organization, *i.e. composite rating*, using the information discussed in limitations 1[a] through 1[c]. Specifically Tippetts discloses a “security risk index determining module [which] determin[es] the security risk index” and that it is a “software module[] running in a distributed computing environment,” *i.e. processing by computer*. Tippetts at ¶¶29-30. Tippetts further discloses that the “security risk index

... may be a local security risk index representing the security of ... information resources associated with the entity,” *i.e. a composite rating of the organization*. *Id.* at ¶45. As discussed above for limitations 1[a] and 1[c], the “local security risk index” is calculated by using various information related to the security and resilience of the network.

137. With respect to the limitation “*the composite rating comprising a calculated composite of metrics and data derived or collected from the sources*,” Tippet explains that the “local security risk index” is “expressed as $LSRI = GT \cdot LV \cdot GI$ where GT may be associated with a general threat factor, LV may be associated with a local vulnerability factor, and GI may be associated with a general impact factor.” *Id.* at ¶47. It is the “local vulnerability factor” which is calculated using the above information discussed in limitations 1[a] through 1[c] (which as discussed in limitation 1[e] is *collected from information sources*) by weighing the various pieces of information to form a *composite rating*. *Id.* at ¶¶49-53. One component of calculating the local vulnerability factor involves calculating various “local vulnerability factor components” where each one is calculated using the below equation:

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

Id. at ¶52. Each LVFC “represent[s] the valuated local vulnerability factor component for the specific type of security event, and $E_1 - E_n$ may represent probabilities that the various one or more implemented mitigating measures will

prevent the specific type of security event from causing a breach of security.” *Id.* at ¶53. Thus, the local vulnerability factor is a ***composite of metrics and data***, such as metrics about mitigating measures and data about which mitigating measures have been implemented and which security events the entity has seen. Other information discussed in limitations 1[a] and 1[c] are also other forms of ***metrics and data***.

138. In addition, the “general threat factor” and “general impact factor,” which are used to calculate the “local security risk index,” are calculated using information from the information sources 242, and are therefore ***a calculated composite of metrics and data from the information sources***. Tippet at ¶37 (“The general threat factor component gathering operation 312 may include obtaining data from the plurality of information sources 242”), ¶43 (“The at least one general impact factor component may include information located on the at least one information source 242”).

139. With respect the limitation ***“indicative of a degree of risk to the organization or to a party through a business relationship with the organization,”*** Tippet teaches that a security risk index, including a local security risk index, can be compared to a “certification value” to provide “an object security goal.” *Id.* at ¶62. If the entity is certified, it allows the entity “to verify to outside parties such as clients, partners, insurers, vendors, consultants, associates, competitors, or other parties, that the specific subset of information resources associated with the entity 224A is secure.”

Id. Thus, the local security risk index is *indicative of a degree of risk to the organization's business partners*.

9. 1[i]: the processing comprising applying transformations to the data and metrics, and the processing comprising applying weights to the data and the metrics,

140. Tippettt teaches that the local security risk index is calculated by applying *transformations and weights* to the data and metrics. For example, Tippettt discloses that the “local vulnerability factor component[s]” which are used to calculate the “local security risk index” are “weighted based on an effectiveness of a mitigating measure designed to secure information resources that has been employed by the entity 224A, a past rate of success for a specific type of security event against the entity 224A, a rate or frequency at which a specific type of security event experienced by the entity 224A, or any other appropriate feature,” *i.e. applying weights to the data and the metrics*. Tippettt at ¶50.

141. In addition, the local vulnerability factor components can be calculated using the below equation, where “LVFC may represent the valuated local vulnerability factor component for the specific type of security event, and E_1 – E_n may represent probabilities that the various one or more implemented mitigating measures will prevent the specific type of security event from causing a breach of security,” *i.e. a transformation to the data and metrics*. Tippettt at ¶53.

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

142. In addition, Tippet discloses that the components used to calculate the “general threat factor” and the “general impact factor” are normalized and weighted, *i.e. applying transformations and weights to the data and metrics*. Tippet at ¶¶38-39, 44.

10. 1[j]: the metrics including a measure of the extent of, the frequency of, or duration of compromise of the technology systems of the organization, or of a configuration or vulnerability of the organization, and a measure of the resilience of the organization to recover from such vulnerability, the measure of the resilience being inversely proportional to the duration of detected malicious activity, and

143. With respect to the limitation “*the metrics including a measure of the extent of, the frequency of, or duration of compromise of the technology systems of the organization, or of a configuration or vulnerability of the organization,*” as discussed above for limitation 1[b], Tippet discloses gathering various kinds of information, such as “a rate or frequency at which a specific type of security event [was] experienced by the entity,” *i.e. the frequency of compromise of the technology systems of the organization*. Tippet at ¶50. Tippet also discloses metrics regarding “a past history of at least one type of security breach,” *i.e. extent of compromise*. *Id.* at ¶49. Finally, as discussed above for limitation 1[c], Tippet discloses (or renders obvious alone or in combination with McGovern) a *measure of the duration of compromise*.

144. With respect to the limitation ***“and a measure of the resilience of the organization to recover from such vulnerability, the measure of the resilience being inversely proportional to the duration of detected malicious activity,”*** as discussed above for limitation 1[c], Tippet discloses using a measure of “an effectiveness of a mitigating measure designed to secure information resources that has been employed by the entity.” Tippet at ¶50. Tippet further describes that the mitigating measure includes “a detection aspect” and “a recovery aspect,” which indicates that it is a ***measure of resilience to recover from such vulnerability.*** Tippet at ¶52.

145. As also discussed in limitation 1[c], a POSITA would understand and consider it obvious that this measure of effectiveness includes the ***duration of detected malicious activity***, such the “detection aspect” and “recovery aspect” together would compromise the duration. Furthermore, McGovern discloses “average response or patch time after security breach detection,” which could be incorporated into Tippet as its effectiveness measure using the detection and recovery aspects of the mitigating measure. McGovern at ¶38; Tippet at ¶52. A POSITA would understand that the effectiveness of a mitigating measure would involve minimizing the “response or patch time” (for all the reasons discussed in limitation 1[c]) and therefore would be ***inversely proportional to the duration of detected malicious activity.***

11. 1[k]: in connection with assessing a business risk to the organization or to a party through a business relationship with at least one of the organizations, delivering reports of the composite ratings of the organizations through a

reporting facility to enable users of the reporting facility to monitor, assess, and mitigate the risks, based on the security vulnerabilities and resiliencies, in doing business with the organization and to compare the composite ratings of the organizations.

146. With respect to the limitation *“in connection with assessing a business risk to the organization or to a party through a business relationship with at least one of the organizations,”* as discussed above for limitation 1[h], Tippet discloses a “local security risk index” which is used to *assess a business risk to a party in a relationship with an entity, i.e. organization.*

147. With respect to the limitation *“delivering reports of the composite ratings of the organizations through a reporting facility,”* Tippet discloses a “graphical representation,” *i.e. reporting facility*, of “first local security risk index” and a “second local security risk index,” each for a different entity, *i.e. reports of the composite ratings of the organizations.* Tippet at ¶57. Tippet also discloses that the “reporting of a security risk index” can include a “quality level,” which represents the “level of preciseness.” *Id.* at ¶56.

148. With respect to the limitation *“to enable users of the reporting facility to monitor, assess, and mitigate the risks, based on the security vulnerabilities and resiliencies, in doing business with the organization,”* Tippet discloses that the graphical representation allows users to *monitor, assess, and mitigate risks in doing business with the entity.* For example, Tippet discloses that, through the graphical

representation (*i.e. reporting facility*), a user can observe “effectiveness of at least one mitigating measure ... by comparing” a local security risk index before and after the mitigating measure is implemented. Tippet at ¶60 (“trends in the security of ... the entity 224A may be monitored over time by observing the first local security risk index 614 over time.”). By observing the effectiveness of the mitigating measure, the user ***monitors and assess the risk*** of vulnerabilities on the entity’s network. The local security risk index can also be reported as a “certification of the security of ... the entity,” which “verif[ies] to outside parties such as clients ... that the ... entity 224A is secure.” *Id.* at ¶62. In addition, Tippet discloses a “security threshold” which the security risk index must meet before allowing “connecting to ..., downloading..., [or] opening ... the information resources,” thereby mitigating risk in doing business (*e.g.* connecting to, downloading, opening) with the entity and its network. Tippet at ¶63. Thus, the ***reporting facility*** also allows users to ***mitigate risks*** such as by a client requiring that the organization provide certification before engaging in business.

149. A POSITA would understand that risks of vulnerabilities and malicious activity on the entity’s network is a ***risk in doing business with the entity***, especially in view of Tippet’s disclosure that “clients, partners, insurers, vendors, consultants, associates,” etc. would desire “verif[ication]” that the organization’s network is secure. Tippet at ¶62. A POSITA would understand that this is because such parties may involve exchange of confidential or sensitive information while doing

business with the entity, and thus would understand that the risk of vulnerabilities or malicious activity wherein the business partner's data may be misappropriated is also *a risk in doing business with the entity*.

150. With respect to the limitation “*and to compare the composite ratings of the organizations,*” Tippet discloses that the graphical representation allows a user to “compar[e] the first local security risk index 614 of the specific subset of information resources associated with the entity 224A [*i.e. composite rating of first organization*] with the second local security risk index 616 of the specific subset of information resources associated with the other entity [*i.e. composite rating of second organization*].” Tippet at ¶58.

C. Claim 2: The method of claim 1, wherein the collected information is represented by at least two data types.

Claim 3: The method of claim 2, wherein the at least two data types include at least one of breach disclosures, block lists, configuration parameters, an identification of malware servers, an identification of a reputation, an identification of suspicious activity, an identification of spyware, white lists, an identification of compromised hosts, an identification of malicious activity, an identification of spam activity, an identification of vulnerable hosts, an identification of phishing activity, or an identification of e-mail viruses.

151. In my opinion, Tippet alone discloses or in combination with McNab renders obvious that the collected information discussed in limitations 1[a] through 1[c] is represented by at least the data types *breach disclosures, identification of suspicious activity, identification of vulnerable hosts* and *identification of malicious*

activity. For example, Tippet discloses that the information comprises “a past history of at least one type of security breach,” *i.e.* a ***breach disclosure***. Tippet at ¶49. Tippet also discloses that the information comprises “a type of possible security breach that is unique to ... the entity,” *i.e.* ***identification of vulnerable hosts***, since a POSITA would understand that identifying a ***type*** of security breach unique to the entity would involve identifying which hosts are vulnerable to the security breach—for example, an unpatched vulnerability would indicate a type of security breach unique to the entity.

152. In addition, as discussed above for limitation 1[b], McNab discloses the ability to scan for ***suspicious and malicious activity***, such as the presence of the “MS Blaster worm” or other viruses. Exs. 1008, 1009.

D. Claim 4: The method of claim 1, wherein the collected information evidences internal security controls.

153. Tippet alone discloses or in combination with McNab renders obvious that the collected information discussed in limitations 1[a] through 1[c] is ***evidence of internal security controls***. For example, Tippet discloses that collected information comprises “certain mitigating measures designed to secure information resources that is unique to ... the entity,” “a future plan for securing the information resources associated with the entity,” “effectiveness of a specific implemented mitigating measure to safeguard information resources against a specific type of security event,” and “mitigating measures [that] will prevent the specific type of security event from causing a breach of security.” *Id.* at ¶¶49-51, 53. Similarly, McNab discloses

collecting information such as the presence of antivirus software. Ex. 1023. All of these are *evidence of internal security controls*.

E. Claim 5: The method of claim 1, wherein the collected information comprises outcomes of each of the organizations.

154. Tippet discloses that collected information discussed in limitations 1[a] through 1[c] *comprises outcomes of an organization*. For example, Tippet discloses collecting information related to “a past history of at least one type of security breach,” “a rate or frequency at which a specific type of security event [was] experienced by the entity,” and the “effectiveness of a specific implemented mitigating measure to safeguard information resources against a specific type of security event.” *Id.* at ¶¶49-50. Such information is indicative of *outcomes* like the outcome of breaches, exploitation of vulnerabilities, and mitigating measures against security events.

155. As also discussed above, Tippet discloses that a local security risk index is calculated for each entity, *i.e. an organization*, and thus a POSITA would understand that the collected information used to calculate a local security risk index is for *each of the organizations*. See Tippet at ¶46.

F. Claim 6: The method of claim 1, wherein the collected information evidences operational execution of security measures of each of the organizations.

156. Tippet discloses that collected information discussed in limitations 1[a] through 1[c] *is evidence of operational execution of security measures*. For

example, Tippet discloses that collected information includes “effectiveness of a specific implemented mitigating measure to safeguard information resources against a specific type of security event” and “a past rate of success for a specific type of security event against the entity.” Tippet at ¶¶50-51.

157. As also discussed above, Tippet discloses that a local security risk index is calculated for each entity, *i.e. an organization*, and thus a POSITA would understand that the collected information used to calculate a local security risk index is for *each of the organizations*. See Tippet at ¶46.

G. Claim 7: The method of claim 1, wherein the collected information indicates whether a computer system of each of the organizations served malicious code to another system.

158. Tippet in view of McNab renders obvious that the collected information *indicates a computer served malicious code to another*. For example, McNab discloses the ability to detect that “[t]he remote host [is] infected by the MS Blaster worm.” Ex. 1008. A POSITA would understand that worms, such as the MS Blaster worm, spread by *serving malicious code to another system*, specifically by sending malicious code to the Windows RPC service running on computers at randomly generated IP addresses. See Ex. 1022. Thus, if a computer system is infected, then it would have served said malicious code to another system.

159. As also discussed above, Tippet discloses that a local security risk index is calculated for each entity, *i.e. an organization*, and thus a POSITA would

understand that the collected information used to calculate a local security risk index is for *each of the organizations*. See Tippet at ¶46.

H. Claim 8: The method of claim 1, wherein the collected information indicates whether a computer system of each of the organizations communicated with a known attacker controlled network or sensor outside the control or network of the organization.

160. Tippet in view of McNab renders obvious the collection of information indicating, through the presence of certain malware like W32.SoBig, that a computer *communicated with a known attacker controlled network outside the control or network of the organization*. As discussed above in limitation 1[c], McNab describes using the Nessus vulnerability scanner, which includes a plug-in for detecting the W32.SoBig worm in a remote host. Ex. 1009. The W32.SoBig worm was known to contact various IP addresses controlled by the attacker to download additional programs, such as the WinGate proxy server software that allowed an attacker to control the infected computer system. Ex. 1024. As a result, detecting the presence of W32.SoBig would be an indication that the computer system *communicated with a known attacker controlled network*.

161. As also discussed above, Tippet discloses that a local security risk index is calculated for each entity, *i.e. an organization*, and thus a POSITA would understand that the collected information used to calculate a local security risk index is for *each of the organizations*. See Tippet at ¶46.

162. As an aside, it is my opinion that Exhibit 1024 was publicly available by 2003. Exhibit 1024 is an article published in IEEE Security & Privacy on 2003. I am familiar with the IEEE's publication practices, having published in many IEEE journals. The IEEE is a renowned and reputable publisher of scientific and technical articles, and the dates listed on their papers are a strongly reliable indicator of its public availability. In fact, I understand that the Board has stated that the IEEE is a well-known, reputable compiler and publisher of scientific and technical publications, and that POSITAs rely on the copyright date provided in IEEE publications. I agree with the Board.

163. I further note that Exhibit 1024 is listed on the IEEE Xplore website at <https://ieeexplore.ieee.org/document/1219071>, with a date of publication of August 11, 2003. A POSITA would also consider the IEEE Xplore website as a highly reliable date indicative of publication status. In my opinion, Exhibit 1024 is also a complete, true, and correct copy, since it is identical to the copy available on IEEE Xplore. Exhibit 1024 is complete and has no visible alterations. The IEEE Xplore database is exactly the place an IEEE-published paper would appear. Exhibit 1024 also has all the hallmarks of an authentic copy of an IEEE-published paper, IEEE markings, a stylized title, and a blurb about the author at the end.

I. Claim 9: The method of claim 1, comprising: forming a series of the security ratings of each of the organizations.

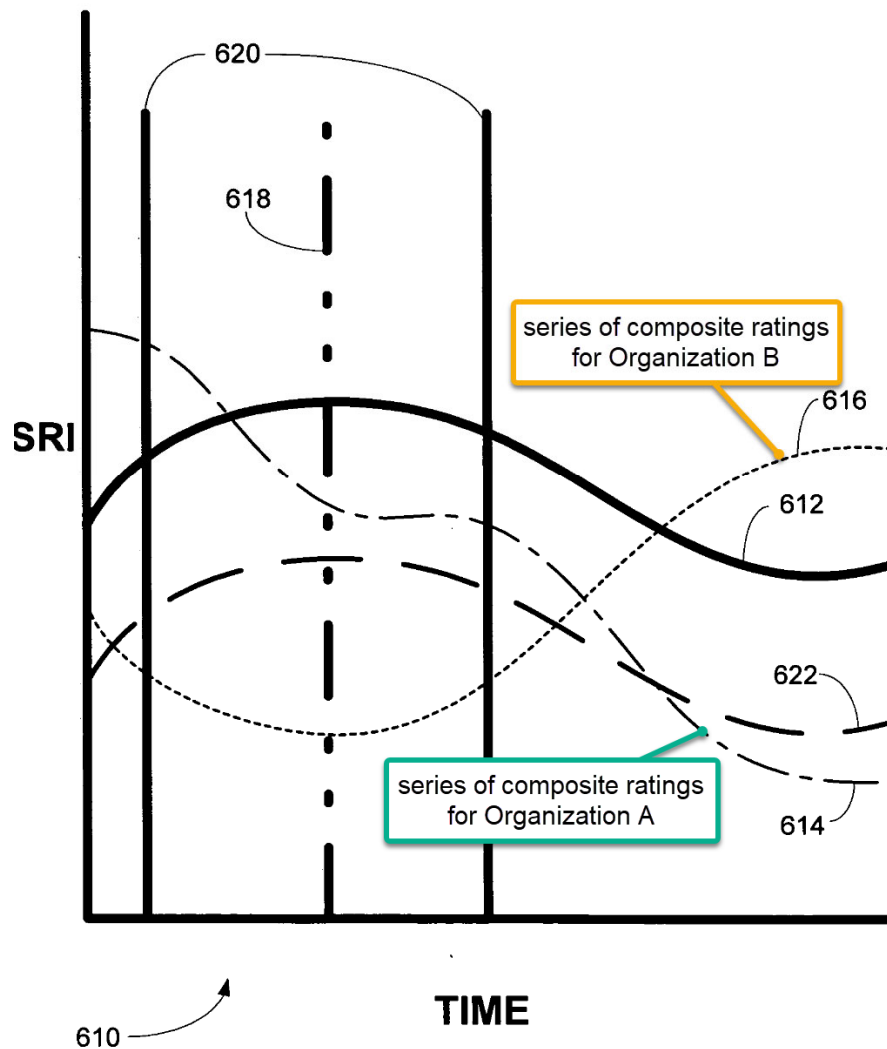
Claim 10: The method of claim 9, comprising: determining a

trend from the series of ratings.

Claim 11: The method of claim 9, comprising displaying the series of composite ratings.

164. Tippet discloses a “graphical representation” of local security indexes, *i.e. security ratings*, for each organization over time. Tippet at ¶57; Fig. 6 (annotated below). Thus, Tippet discloses *forming and displaying a series of composite ratings*. Tippet also discloses *determining a trend from the series*, specifically that determining “effectiveness of at least one mitigating measure” by looking at the trend of the security risk index before and after implementation of the mitigating measure. *Id.* at ¶60. Tippet also discloses “*trends in the security of the specific subset of information resources* associated with the entity 224A may be monitored over time by observing the first local security risk index 614 over time.” *Id.*

FIG. 6



- J. Claim 12: The method of claim 11, wherein displaying the series of composite ratings for each of the organizations comprises posting the series of composite ratings for the organization to a web portal.**

165. Tippet in view of McGovern renders obvious *posting the series of composite ratings for the organization to a web portal*. In particular, McGovern teaches calculating security assessment scores wherein users can “*access the scoring*

and related functionalities *remotely via standard browsers* or similar *user interfaces*.”

McGovern at ¶45. A POSITA would understand that accessing remotely via a web browser means the browser is accessing a web portal. As discussed above, a POSITA would have found it obvious to combine Tippet with McGovern’s teachings of a web portal user interface.

K. Claim 13: The method of claim 1, wherein the collected information represents externally observable outcome information.

166. Tippet in view of McNab renders obvious that the collected information *represents externally observable outcome information*. As discussed in limitation 1[b], McNab discloses a Nessus vulnerability scanner that can, from outside the network, scan for the presence of viruses or the presence of antivirus software. Exs. 1008, 1009, 1023. Such information is *externally observable information* and represents the *outcome* of some security event, such as whether a vulnerability was exploited, resulting in the installation of malware of a virus, or the installation of a mitigating measure such as antivirus software. These are *outcome information* about some security event.

L. Claim 14: The method of claim 1, comprising: determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information.

167. Tippet discloses a calculation of a local vulnerability factor component (“LVFC”), *i.e. a badness score*, that is calculated using the following

formula, wherein “ E_1 - E_n may represent probabilities that the various one or more implemented mitigating measures will prevent the specific type of security event from causing a breach of security,” which *corresponds to an intensity of malicious activity* because the probability of prevention inversely correlates with the actual fact of a particular security event, and therefore the *intensity of different types of malicious activity as a whole*. Tippet at ¶53.

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

M. Claim 15: The method of claim 1, wherein: the collected information comprises at least two security characterizations of a computer system of each of the organizations.

168. Tippet discloses and in view of McNab renders obvious that collected information discussed in limitations 1[a] through 1[c] *comprises at least two security characterizations of a computer system*. For example, Tippet discloses that collected information includes “a past rate of success for a specific type of security event against the entity” and the “effectiveness of a specific implemented mitigating measure to safeguard information resources against a specific type of security event.” Tippet at ¶¶49, 50. A “security event” includes “any event that threatens the security of one ... information resource[],” *i.e. a computer system*. Thus, such information are *security characterizations of a computer system*.

169. In addition, as discussed above for limitation 1[b], McNab discloses using the Nessus vulnerability scanner to determine the presence of malware like the

MS Blaster worm or the W32.SoBig worm on a “remote host.” Exs. 1008, 1009. McNab also discloses determining the presence of antivirus software on a remote host. Ex. 1023. These are also *security characterizations of a computer system*.

170. As also discussed above, Tippet discloses that a local security risk index is calculated for each entity, *i.e. an organization*, and thus a POSITA would understand that the collected information used to calculate a local security risk index is for *each of the organizations*. See Tippet at ¶46.

N. Claim 16: The method of claim 1, wherein the collected information comprises a characterization of behavior of an employee of at least one of the organizations.

171. Tippet discloses collecting information about “security events” which includes “any event that threatens the security of one or more information sources.” *Id.* at ¶37. A POSITA would understand that this information would therefore include susceptibility to social engineering attacks which is a *characterization of behavior of employees*, because social engineering involves tricking employees of an organization to give up information or provide access, such as a phishing attack. A phishing attack is often sent via email that tricks an employee to click or download malware by, for example, pretending to be a trustworthy source. Phishing attacks were well-known. One example of a phishing attack that was known is an email to an employee that is intended to mimic the organization’s IT administrator seeking access credentials.

O. Claim 17: The method of claim 1, wherein the collected information comprises characterizations other than

characterizations about a computer system of at least one of the organizations.

172. Tippet discloses that collected information discussed in limitations 1[a] through 1[c] *includes characterizations that are not about a computer system*. For example, Tippet discloses that collected information includes “effectiveness of a mitigating measure designed to secure information resources that has been employed by the entity.” Tippet at ¶50. A POSITA would understand that such information is a characterization of a *mitigating measure*, which could include policies that are not about a particular computer system, such as policies about personal email usage.

173. In addition, Tippet discloses collecting information about “future security events discovered in chat rooms or on message boards,” which is included in the calculation of the “general threat factor” used to calculate the “local security risk index,” and thus would be included in the collected information claimed in limitations 1[a] through 1[c]. Tippet at ¶¶37, 47. Such information is *not about a computer system of the organization* since it is about future security events.

174. As also discussed above, Tippet discloses that a local security risk index is calculated for each entity, *i.e. an organization*, and thus a POSITA would understand that the collected information used to calculate a local security risk index is for *each of the organizations*. See Tippet at ¶46.

P. Claim 18: The method of claim 1, wherein the collected information comprises characterizations about policies of at least one of the organizations.

175. As discussed above for limitation 1[b], Tippet discloses that it collects information “a future plan for securing the information resources associated with the entity,” *i.e. characterizations about policies of an organization*. Tippet at ¶49. A future security plan for the entity’s assets is a *policy* of an organization.

Q. Claim 19: The method of claim 1, wherein the collected information comprises characterizations about information technology assets that at least one of the organizations owns, controls, uses, or is affiliated with.

176. As discussed above for limitation 1[f], which recites “gathering information about assets that each of the organizations owns, controls, uses, or is affiliated with,” Tippet discloses and in view of McNab renders obvious this limitation, since the information described above are *characterizations of such assets*.

R. Claim 20: The method of claim 1 in which collected information represents: (a) physical states, (b) technical states, (c) organizational states, or (d) cultural states of at least one of the organizations which can be exploited to create a security breach; or (e) the organization's ability to recover from a security breach; or any combination of two or more of these.

177. As discussed above for limitation 1[b], Tippet discloses information that represents *the organization’s ability to recover from a security breach*. In particular, Tippet discloses that the information constitutes “effectiveness of the specific implemented mitigating measure” which includes “a *recovery* aspect.” Tippet at ¶52. In addition, as discussed above for limitation 1[b], McNab discloses collecting

information representing *technical states* of the organization, such as the presence of viruses or antivirus software.

S. Claim 21: The method of claim 1 in which processing the information to form a composite rating comprises correlating data across the sources of information.

178. Tippetts discloses the use of “probabilities that the various one or more implemented mitigating measures will prevent the specific type of security event from causing a breach of security.” Tippetts at ¶53. Such probabilities involve *correlating data across the sources of information*, since it correlates mitigating measures with probabilities of certain outcomes. For example, a POSITA would understand that in order to evaluate probabilities that a mitigating measure will prevent a security event, one would need information from different organizations that indicate whether or not the mitigating measure was effective and preventing a security event. Such information would come from different sources of information, and in compiling these probabilities, the effectiveness of the mitigating measure for each organization will be correlated to calculate the probability.

T. Claim 22: The method of claim 1 in which processing the information to form a composite rating comprises statistically correlating the composite rating with actual outcomes.

179. Tippetts discloses that the security risk index, *i.e. composite rating*, is *statistically correlated with actual outcomes*. Specifically, Tippetts discloses that the security risk index “may be expressed as $SRI = T * V * I$, where T may represent a threat

factor associated with a rate or frequency of security events that threaten the security of the information resources.” Tippet at ¶23. Thus, the security risk index is *correlated with* a threat factor which measures *actual outcomes of security events*.

U. Claim 23: The method of claim 1 in which the vulnerability comprises physical, technical, organizational, or cultural states that can be exploited to create a security breach.

180. Tippet discloses that information indicative of vulnerabilities includes “a type of possible security breach that is unique to ... the entity.” Tippet at ¶48. A POSITA would understand that such information is indicative of at least *technical or organizational states that can be exploited*, because it is a security breach unique to the *entity*, *i.e.* the organization. The information therefore indicates that the entity or the technical assets of the entity are in a particular state that allows them to be uniquely exploited to create a security breach.

V. Claim 24

1. 24[pre]: A method comprising:

181. *See* limitation 1[pre].

2. 24[a]: collecting, from at least two sources, information about two or more organizations, the collected information representing at least two data types, the collected information comprising outcomes of each of the organizations,

182. Limitation 1[a] recites “collecting information about two or more organizations,” which is recited in this limitation.

183. Limitation 1[e] recites “the information about each of the organizations being collected from two or more sources,” which is identical to “collecting, from at least two sources.”

184. Claim 2 recites “the collected information is represented by at least two data types,” which is recited in this limitation.

185. Claim 5 recites “the collected information comprises outcomes of each of the organizations,” which is recited in this limitation.

186. Thus, Tippet in view of McNab and McGovern render obvious this limitation for the same reasons discussed above for limitations 1[a], 1[e] and claims 2 and 5.

3. 24[b]: at least some of the information for each of the organizations being collected automatically by computer from at least two sources, one or more of the sources not controlled by the organization,

187. Limitation 1[d] recites “at least some of the information about each of the organizations being collected automatically by computer,” which is recited in this limitation.

188. Limitation 1[e] recites “the information about each of the organizations being collected from two or more sources, one or more of the sources not being controlled by the organization,” which is substantively identical to the limitation “information ... collected ... from at least two sources, one or more of the sources not controlled by the organization.”

189. Thus, Tippet in view of McNab and McGovern render obvious this limitation for the same reasons discussed above for limitations 1[d] and 1[e].

4. **24[c]: the information from at least the one or more sources that are not controlled by the organization being collected without permission of the organization, at least one of the sources including a commercial data source,**

190. Limitation 1[e] recites “the information from at least the one or more sources that are not controlled by the organization being collected without permission of the organization,” which is recited in this limitation.

191. Limitation 1[g] recites “at least one of the sources for each of the organizations comprising ... a commercial source,” which is substantively identical to this limitation.

192. Thus, in my opinion, Tippet in view of McNab and McGovern render obvious this limitation for the same reasons discussed above for limitations 1[e] and 1[g].

5. **24[d]: processing the information from both of the two sources for each of the organizations to form a composite rating of a security vulnerability of the organization and of a resilience of the organization to recover from a security breach, the resilience being inversely proportional to the duration of detected malicious activity, the processing including applying models that account for differences in the respective sources,**

193. Limitation 1[h] recites “processing by computer the information from the two or more sources for each of the organizations to form a composite rating” and

limitation 1[j] recites “the metrics including a measure of the extent of ... vulnerability of the organization ... and a measure of the resilience of the organization to recover from such vulnerability, the measure of the resilience being inversely proportional to the duration of detected malicious activity.” Together, these limitations are substantively identical to this limitation save for the additional limitation of “the processing including applying models that account for differences in the respective sources.” Thus, in my opinion, Tippet in view of McNab and McGovern render obvious this limitation for the same reasons discussed above for limitations 1[h] and 1[j].

194. Tippet also discloses that generating the local security risk index involves weighting certain components by *applying a model based on the differences in the respective sources*. Specifically, Tippet discloses that generating the local security risk index involves calculating a “general threat factor” which involves gathering “general threat factor *component[s]*.” Tippet at ¶¶47, 37. Each general threat factor component involves obtaining data from an “information source[],” *i.e. respective sources*, which results in each component having different forms, be that “a rate, a frequency, a count, a scale, or another form.” *Id.* at ¶38. A POSITA would understand that the form of the data is dependent on the differences in data forms in the respective sources—for example, one information source may offer data that is a rate, another information source may offer data that is a scale. In order to account for

the differences in the data forms that is a result of *differences in the respective sources*, Tippet discloses “convert[ing]” each component “into a common format, and to rank the at least one general threat factor component based on, for example, 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.” *Id.* at ¶38. A POSITA would understand that “conver[sion] ... into a common format” would involve using a model that applies mathematical transformations and weights dependent on the data type being converted. *Id.*

6. 24[e]: normalizing the composite rating of each of the organizations based on a size characteristic of the organization to enable comparisons of composite ratings between the two or more organizations,

195. Tippet discloses that comparisons of local security risk indices accounts for differences in the size of the entities being compared. Specifically, Tippet discloses that, when comparing a local security risk index for one entity against that of another, the comparison can be made “despite at least one difference between ... the entities.” Tippet at ¶58. One difference that is accounted for is “a difference in the *sizes of the*” two entities being compared. *Id.* A POSITA would understand that in order to account for size differences between two entities, the local security risk indices would need to be *normalized based on size of the entities*. For example, one piece of information used to calculate a local security risk index is the “frequency at which a specific type of security event experienced by the entity.” *Id.* at ¶50. A larger entity is

likely to have a higher frequency of security events than a smaller entity because a larger entity will have more network assets and more valuable data to misappropriate. In order to compare the local security risk index of a larger entity against that of a smaller entity, “despite ... a difference in the sizes” of the two, the local security risk index would need to be normalized to allow for a user to make a proper comparison. *Id.* at ¶58. Without said normalization, the local security risk index of the smaller entity would appear smaller than the local security risk index of the larger entity even if the larger entity’s network is more secure. This would confuse and mislead the user. For these reasons, a POSITA would also consider it obvious to normalize the local security risk indices to account for size in order to avoid misleading or confusing the user and to give effect to Tippet’s instruction that comparison of the two should account for differences in the sizes of the entities. A POSITA would have a reasonable expectation of success because normalizing the indices would be well-within the skill of a POSITA—a simple method would divide a scalar value by the size of entity to produce a rate. A more complex method but still well-within the capabilities of a POSITA would take past data and generate a best-fit curve.

7. **24[f]: forming a series of the security ratings of each of the organizations, determining a trend from the series of ratings, and displaying the series of composite ratings through a portal,**

196. Claim 9 recites “forming a series of the security ratings of each of the organizations.”

197. Claim 10 recites “determining a trend from the series of ratings.”

198. Claim 11 recites “comprising displaying the series of composite ratings.”

199. Together, these claims recite this limitation and thus Tippet in view of McNab and McGovern render obvious this limitation for the same reasons discussed above for Claims 9, 10, and 11.

8. 24[g]: determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information, and

200. Tippet in view of McNab and McGovern render obvious this limitation for the same reasons discussed above for Claim 14.

9. 24[h]: reporting the composite ratings of the organizations through a portal to enable customers to monitor, assess, and mitigate risk in doing business with the organizations and to compare the composite ratings across the organizations.

201. Tippet in view of McNab and McGovern render obvious this limitation for the same reasons discussed above for limitation 1[k].

W. Claim 25: The system of claim 24, determining a confidence range of the composite rating, the size of the range varying inversely with the level of confidence in the composite rating.

202. Tippet discloses that the local security risk index, *i.e. composite rating*, has a preciseness, *i.e. a confidence range*, that varies with the confidence of the security risk index. Specifically, Tippet discloses that “[a] preciseness of a security risk index may depend on an amount of factor components used” and that “[a] greater

number of factor components may produce a more precise security risk index.” Tippet at ¶56. Tippet discloses an example where the preciseness is categorized into four levels of “Quality,” which are a *level of confidence* in the security risk index. As depicted in Figure 5, the preciseness results in a *confidence range* of the security risk index. For example, a preciseness of “B Quality” results in a range of “+/- 10%,” whereas a preciseness of “C Quality” results in a range of “+/- 20%.” Tippet at Figure 5; *see also* ¶56 (“[P]reciseness may be represented ... by reporting a security risk index using ... a *range of numbers*.”).

		512	514	516	518
		A Quality	B Quality	C Quality	D Quality
520	Precicesness	+/- 0%	+/- 10%	+/- 20%	+/- 30%
522	Sample SRI	2,132	1900 - 2300	Red >2300; Orange 1500-2200; Yellow 900-1500; Blue <900	Red Orange Yellow Blue
524	Depth of Inquiry	Comp- rehensive compliance evaluation (on site investiga- tion).	Adv. Question- aire, vulnerability tests, and a phone interview.	Standard Question- aire and perimeter vulnerability testing.	Superficial inquiry.

203. As can be seen from Figure 5, the *confidence range varies inversely* with the level of preciseness quality, *i.e. level of confidence in the composite rating*.

X. Claim 26: The system of claim 25, wherein the confidence range is based on redundancy of the security characterizations.

204. Tippet discloses that the SRI preciseness, *i.e. confidence range*, is based on the number of factor components, *i.e. redundancy of the security characterizations*. Tippet at ¶56. Tippet lists a number of factor components, some of which are similar and therefore provide *redundancy of the security characterizations*. For example, Tippet discloses that a local vulnerability factor component could include both “effectiveness of a mitigating measure designed to secure information resources that has been employed by the entity” and “effectiveness of a specific implemented mitigating measure to safeguard information resources against a specific type of security event.” Tippet at ¶¶50-51. Such factor components provide a level of redundancy of the security characterizations and including both will increase the preciseness quality and decrease the *confidence range*.

Y. Claim 27: The system of claim 25, wherein the confidence range is based on a size of the third party computer system.

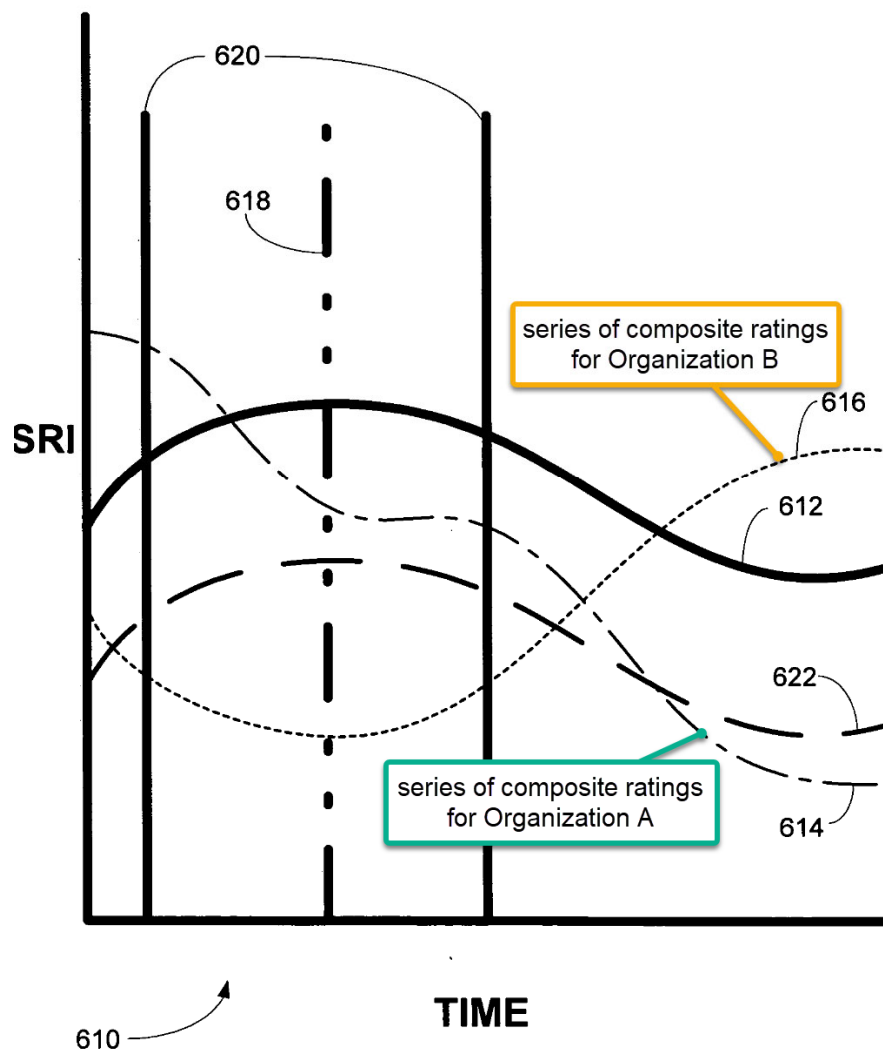
205. I note that neither claims 24 or 25 have an antecedent basis for “third party computer system.” Without conceding that it has an antecedent basis, if “third party computer system” is held to refer to claim 24’s “computer from at least two sources,” Tippet discloses this limitation, particularly that the “preciseness of a security

risk index [*i.e.* **confidence range**] may depend on an amount of factor components” where “[a] greater number of factor components may produce a more precise security risk index than a smaller number of factor components.” Tippet at ¶56. Thus, the confidence range is based on the amount of factor components which is indicative of the size of the *third party computer system*.

Z. Claim 28: The method of claim 1 comprising ranking the organization and other organizations within sectors or peer-groups or globally.

206. Tippet discloses comparing, *i.e.* **ranking**, the local security risk indices of multiple organizations. Specifically, Tippet discloses “a graphical representation” that depicts the relative ranking of local security risk indices for multiple entities, *i.e.* **organizations**. Tippet at ¶57; Fig. 6 (annotated below).

FIG. 6



207. Tippet further discloses that a “group of entities” can constitute “a group of institutions within an industry,” *i.e. organizations within sectors or peer-groups or globally*. Tippet at ¶10.

AA. Claim 29

1. 29[pre]: A method comprising:

208. *See* limitation 1[pre].

2. 29[a]: collecting information about an organization that has computer systems, network resources, and employees, the organization posing risks to itself or to other parties through business relationships of the organization with the other parties,

209. *See* limitation 1[a].

3. 29[b]: the information collected about the organization including (a) information collected automatically by computer on the Internet without permission of the organization, and (b) information indicative of resiliencies of the organization to recover from a security breach associated with a compromise or a vulnerability, the resiliencies being inversely proportional to the duration of detected malicious activity,

210. Limitation 1[d] recites “the information about each of the organizations being collected automatically by computer.”

211. Limitation 1[e] recites “the information ... being collected without permission of the organization.”

212. Limitation 1[b] recites “the information collected about the organizations being ... indicative of resiliencies of the organizations to recover from such compromises, vulnerabilities or configurations.”

213. Limitation 1[j] recites “the resilience being inversely proportional to the duration of detected malicious activity.”

214. Together, the above limitations recite this limitation and therefore Tippet in view of McNab and McGovern renders obvious this limitation for the same reasons discussed above for limitations 1[b], 1[d], 1[e], and 1[j].

4. **29[c]: processing the information by computer to form a composite rating of the organization that is indicative of a degree of risk based on a business relationship with the organization, the composite rating comprising a measure of the resiliencies of the organization to recover from a security breach, and**

215. Limitation 1[h] recites “processing by computer the information ... for each of the organizations to form a composite rating of the organization that is indicative of a degree of risk to the organization or to a party through a business relationship with the organization.”

216. Limitation 1[j] recites “a measure of the resilience of the organization to recover from such vulnerability.”

217. Together, these limitations are substantively identical to this limitation (and in any case, the analysis for limitation 1[j] discusses recovering from security breaches) and thus Tippet in view of McNab and McGovern render obvious this limitation for the reasons discussed above for limitations 1[h] and 1[j].

5. **29[d]: in connection with assessing the degree of risk, delivering a report of the composite rating of the organization through a reporting facility to enable a user of the reporting facility to assess the risks, based at least in part on the resiliencies.**

218. *See* limitation 1[k].

VIII. CONCLUSION

219. I hereby declare that all statements made of my own knowledge are true and that all statements made on information and belief are believed to be true. I further declare that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of the Title 18 of the United States Code and that such willful false statements may jeopardize the validity of this proceeding.

Executed on this September 6, 2024 by:



Kevin C. Almeroth, Ph. D.