Real-Time Massachusetts Data Security Law Monitoring

Leveraging Asset-Based Configuration and Vulnerability Analysis with Real-Time Event Management

February 22, 2011

(Revision 2)

Table of Contents

INTRODUCTION

Tenable Network Security, Inc. serves customers worldwide and each of our customers has a unique set of security, audit and compliance requirements. This paper provides insights on one specific law, Massachusetts 201 CMR 17, which requires protection of the personal information of all Massachusetts residents.

Specifically, this paper describes how Tenable's solutions can be leveraged to help achieve compliance with MA 201 CMR 17 by ensuring that key assets are properly configured and monitored for security compliance. It is crucial to monitor for compliance in a manner as close to real-time as possible to ensure the organization does not drift out of compliance over time. The greater the gap between monitoring cycles, the more likely it is for compliance violations to occur undetected.

WHAT IS MASSACHUSETTS 201 CMR 17?

The state of Massachusetts has taken an important step to protect the personal information of its citizens by passing legislation that requires specific measures to be taken to secure customer data. The law, commonly known as "MA 201 CMR 17", has an effective date of March 1, 2010 and not only affects businesses that operate within Massachusetts state borders but any organization that handles personal information of a Massachusetts resident. According to MA 201 CMR 17:

> *"This regulation implements the provisions of M.G.L. c. 93H relative to the standards to be met by persons who own or license personal information about a resident of the Commonwealth of Massachusetts."*

It must be noted that the scope of the law is not limited to those "persons" who reside in Massachusetts. Instead, **any** person (which is defined in the law as "*a natural person, corporation, association, partnership or other legal entity, other than an agency, executive office, department, board, commission, bureau, division or authority of the Commonwealth, or any of its branches, or any political subdivision thereof*") who receives, stores, maintains, processes or otherwise has access to even one Massachusetts resident's personal information is now legally obligated to protect that information. The steps outlined in MA 201 CMR 17 are not simply suggestions or recommendations; as with any law, there are penalties for failure to comply and ignorance of the law cannot be used as a defense if a violation occurs.

Some businesses are still struggling with the ability to comply with certain aspects of the legislation. While larger businesses may already have many of the law's requirements in place, such as a security training program or a formal written information security plan, many smaller businesses are still trying to determine how to comply with directives such as:

> *"Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information."*

In most cases, achieving compliance with MA 201 CMR 17 will take not only time and effort, but also capital expenses that can affect a business' bottom line.

Under MA 201 CMR 17 subsection 17.04, titled "Computer System Security Requirements", several points address the need for systems to be maintained and monitored:

> *(4) Reasonable monitoring of systems, for unauthorized use of or access to personal information;*
>
> *(6) For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information.*
>
> *(7) Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.*

One of the issues commonly discussed regarding MA 201 CMR 17 has been scalability. For smaller organizations with just a handful of computers, compliance with these points may be as simple as turning on Windows Update for operating system patches, turning on daily automatic updates for antivirus software and spot-checking systems on a monthly basis to ensure that updates are applied. For larger businesses such as banks, hospitals and retail chains, managing hundreds or thousands of computers (as well as their entire network infrastructures) generally requires a full-time IT staff. Monitoring each and every node on the network, in addition to other administrative tasks, is a daunting task. Whether monitoring is performed manually or through automated technology solutions, there is the very real possibility that compliance with MA 201 CMR 17 will incur a significant financial expense.

Another commonly discussed issue in the law is that of "Encryption of all personal information stored on laptops or other portable devices". One school of thought states that personally identifiable information (PII) should never be stored on portable devices in the first place. The law defines PII as:

> *A Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number[…]*

As the following chart shows, that has not been the case historically and will probably not be the case going forward.

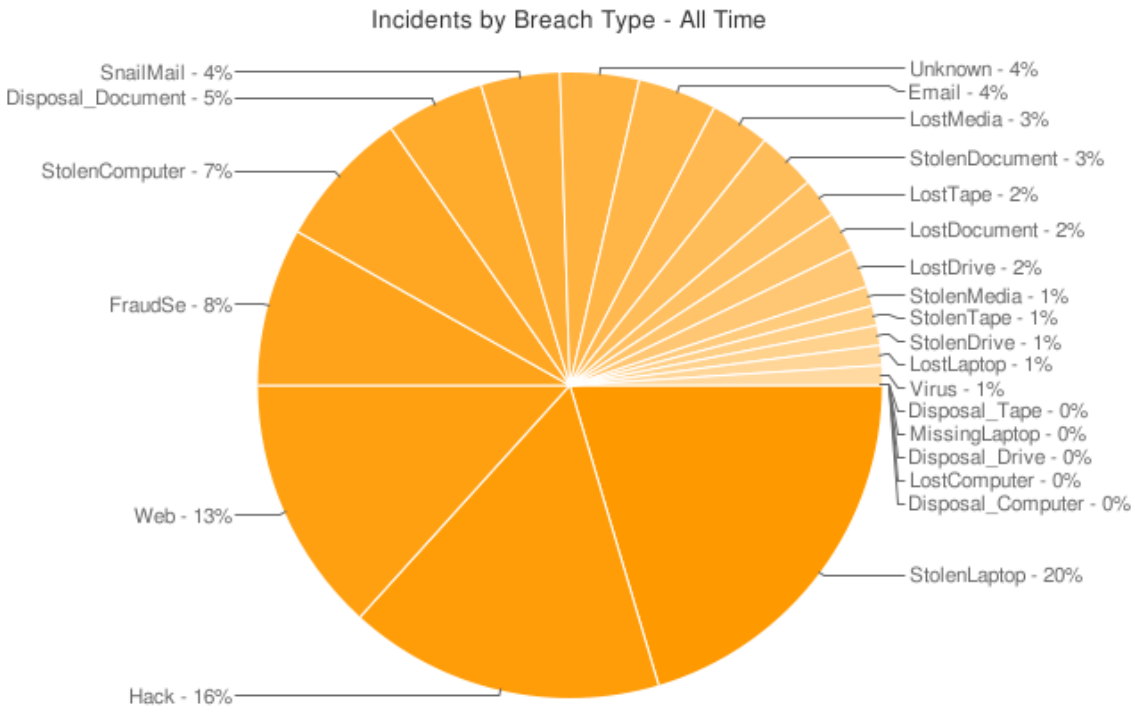

Chart courtesy DataLossDB (http://datalossdb.org/) and the Open Security Foundation

Even though MA 201 CMR 17 addresses encryption of PII on laptops, portable devices and over public and wireless networks, it is useful to know exactly where **all** of your sensitive information resides, regardless of whether it is inside your corporate network or "out in the field". Several state breach notification laws specifically exempt entities from breach notification if it can be proven that lost or stolen data was encrypted. However, you have to know where the data was lost or stolen from in order to know whether or not it was encrypted. All devices containing PII must be inventoried and monitored on a regular basis to ensure compliance with MA 201 CMR 17.

While the list of tasks to accomplish in order to be compliant with MA 201 CMR 17 may appear to be complex, some businesses have found that splitting the task list into technical and non-technical aspects has been to their advantage. Generally non-technical tasks can be found under subsection 17.03: "Duty to Protect and Standards for Protecting Personal Information", and technical aspects are listed under subsection 17:04: "Computer System Security Requirements". Although items such as having a formal written information security program and documenting responsive actions during an incident response may be thought of as non-technical, there are still ways that technology solutions can help with the development of these requirements.

TENABLE'S SOLUTIONS

CORE SOLUTION DESCRIPTION

Tenable offers a Unified Security Monitoring suite of products that can assist in complying with this legislation. Through SecurityCenter, the Log Correlation Engine (LCE) enables you to monitor logs from your assets and alert you when a computer or other device has possibly fallen out of compliance with your security baselines or standards. The Passive Vulnerability Scanner (PVS) continuously monitors traffic across your network, tracks

thousands of client and server application vulnerabilities, detects when new hosts are added to the network and detects which applications and servers host or transmit sensitive data. The Nessus vulnerability scanner performs configuration audits, finds missing patches and upgrades and scans for credit card numbers, Social Security numbers and other types of sensitive information. Together, these products offer a powerful and flexible solution to help ensure compliance with a wide variety of security and compliance standards, as well as regulations and legislation such as MA 201 CMR 17.

Tenable's four basic solutions:

- **SecurityCenter** – Tenable's SecurityCenter provides continuous, asset-based security and compliance monitoring. It unifies the process of asset discovery, vulnerability detection, log analysis, passive network discovery data leakage detection, event management and configuration auditing for small and large enterprises.

- **Nessus vulnerability scanner** – Tenable's Nessus vulnerability scanner is the world-leader in active scanners, featuring high-speed discovery, asset profiling and vulnerability analysis of the organization's security posture. Nessus scanners can be distributed throughout an entire enterprise, inside DMZs and across physically separate networks. Nessus is currently rated among the top products of its type throughout the security industry and is endorsed by professional security organizations such as the SANS Institute. Nessus is supported by a world-renowned research team and has the largest vulnerability knowledge base, making it suitable for even the most complex environments.

- **Log Correlation Engine** – Tenable's Log Correlation Engine (LCE) is a software module that aggregates, normalizes, correlates and analyzes event log data from the myriad of devices within your infrastructure. The LCE can be used to gather, compress and search logs from any application, network device, system log or other sources. This makes it an excellent tool for forensic log analysis, IT troubleshooting and compliance monitoring. The LCE can work with syslog data, or data collected by dedicated clients for Windows events, Netflow, direct network monitoring and many other technologies.

- **Passive Vulnerability Scanner** – Tenable's Passive Vulnerability Scanner (PVS) is a network discovery and vulnerability analysis software solution, delivering real-time network profiling and monitoring for continuous assessment of an organization's security posture in a non-intrusive manner. The PVS monitors network traffic at the packet layer to determine topology, services and vulnerabilities. Where an active scanner takes a snapshot of the network in time, the PVS behaves like a security motion detector on the network.

In addition, Tenable provides SecurityCenter customers with the **3D Tool**, which is designed to facilitate presentations and security analysis of different types of information acquired from SecurityCenter.

The key features of Tenable's products as they relate to compliance auditing are as follows:

Asset Centric Analysis

The combination of network scanning, passive network monitoring and integration with existing asset and network management data allows SecurityCenter to organize network

assets into categories. This enables an auditor to review all components of a particular application.

Typically, an auditor reviews a long list of IP addresses that may have vulnerabilities of various severities associated with them. However, the correlation of interdependencies of an application's components is usually missing. SecurityCenter provides a complete asset list of applications and ensures that the weakest link in the chain is recognized and taken into account.

For example, consider a typical PeopleSoft deployment for a human resources group. The actual PeopleSoft application may run on one or more Windows servers that interact with several databases. It may be connected over some network switches and possibly have front-end web servers for load-balancing. The entire group of servers comprises the "PeopleSoft" asset. A critical security problem in a supporting switch or database can lead to a compromise just as easily as one in the actual PeopleSoft program. It is very efficient for an auditor to be able to work with all of the security issues for one asset type at a time.

Data Leakage Monitoring

Both Nessus and the PVS can identify sensitive data that may be subject to compliance requirements. The Nessus scanner can be easily configured to look for common data formats such as credit card numbers and social security numbers. It can also be configured to search for documents with unique corporate identifiers such as employee names, project topics, sensitive keywords and more. Nessus can perform these searches without a host-based agent and only requires credentials to scan a remote computer.

The PVS can monitor network traffic to identify sensitive traffic in motion over email, web and instant message activity. It can also simply identify servers that host office documents on web servers.

SecurityCenter correlates the information about sensitive data gained from Nessus and the PVS that can be useful in several situations:

- Identifying which assets have sensitive data on them can help determine if data is being hosted on unauthorized systems.
- Classifying assets based on the sensitivity of the data they are hosting can simplify configuration and vulnerability auditing by focusing on those hosts and not the entire network.
- Responding to security incidents or access control violations can be facilitated by knowing the type of information on the target system, which helps identify if a system compromise also involves potential theft or modification of data.

Both Nessus and the PVS also act as a deterrent. If organizations realize they will be audited for their use of certain types of data, they will be more careful in how they transfer and store data.

Configuration Audits

Security policies, guidelines, standards and procedures provide a mandate for maintaining network security. A policy is defined as *what* will and will not be permitted, such as "users are required to have passwords and keep them secure". Guidelines are suggested methods of *how* to adhere to the policy, such as "users should change passwords on a regular basis". Standards are specific *technical rules* for a particular platform, such as Microsoft IIS or

database servers. A standard might state, "passwords must be set to expire every 90 days and must force the user to use a combination of alpha-numeric characters". Finally, procedures provide users and systems administrators with methods for maintaining security, such as "how to install a Microsoft IIS Server Securely". It is important to understand the distinction between these to ensure appropriate compliance.

A configuration audit is one where the auditors verify that servers and devices are configured according to an established standard and maintained with an appropriate procedure. SecurityCenter can perform configuration audits on key assets through the use of Nessus' local checks that can log directly onto a Unix or Windows server without an agent.

There are several audit standards available for SecurityCenter. Some of these come from best practice centers like the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). Some of these are based on Tenable's interpretation of audit requirements to comply with specific industry standards such as PCI DSS, or legislation such as Sarbanes-Oxley.

In addition to the base audits, it is very easy to create customized audits for the particular requirements of any organization. These customized audits can be loaded into SecurityCenter and made available to anyone performing configuration audits within an organization.

Once the audit policies have been configured in SecurityCenter, they can be repeatedly used with little effort. SecurityCenter can also perform audits intended for specific assets. Through the use of audit policies and assets, an auditor can quickly determine the compliance posture for any specified asset.

Security Event Audits

SecurityCenter and the LCE can perform the following forms of security event management:

- Secure log aggregation and storage
- Normalization of logs to facilitate analysis
- Correlation of intrusion detection events with known vulnerabilities to identify high-priority attacks
- Sophisticated anomaly and event correlation to look for successful attacks, reconnaissance activity and theft of information
- Ability to search log data across the enterprise from one central portal
- Ability to identify a particular user's activity across the enterprise based on either IP address or user name

Tenable ships the LCE with logic that can map any number of normalized events to a "compliance" event to support real-time compliance monitoring. For example, a login failure may be benign, but when it occurs on a financial asset, it must be logged at a higher priority. SecurityCenter and the LCE allow any organization to implement their compliance monitoring policy in real time. These events are also available for reporting and historical records.

The LCE also allows for many forms of best practice and Human Resources (HR) monitoring. For example, unauthorized changes can be detected many different ways through network monitoring. Another useful application of the LCE is to determine if users recently separated

from the organization are still accessing the network. All activity can be correlated against user names so that it becomes easy to see who is doing what inside the network.

Tenable's LCE has the ability to store, compress and search any type of ASCII log that is sent to it. Searches can be made with Boolean logic and limited to specific date ranges. There are an infinite number of searches that can be performed, such as searching DNS query records or tracking down known Ethernet (MAC) addresses in switch, DHCP and other types of logs. All search results are saved in a compressed format along with a checksum so that they can be used as forensic evidence if required. Additionally, searches can be saved and then re-launched against the latest log data.

Each LCE can use a local disk store or a mounted file system from a remote NAS or SAN. SecurityCenter can show the disk space usage of each LCE and also predict and alert when it will run out of disk space.

Web Application Scanning

Tenable's Nessus scanner has a number of plugins that can aid in web application scanning. This functionality is useful to get an overall picture of the organization's posture before engaging in an exhaustive (and expensive) analysis of the web applications in the environment. Nessus plugins test for common web application vulnerabilities such as SQL injection, cross-site scripting (XSS), HTTP header injection, directory traversal, remote file inclusion and command execution.

Another useful Nessus option is the ability to enable or disable testing of embedded web servers that may be adversely affected when scanned. Many embedded web servers are static and cannot be configured with custom CGI applications. Nessus provides the ability to test these separately to save time and avoid loss of availability of embedded servers.

Nessus provides the ability for the user to adjust how Nessus tests each CGI script and determine the duration of the tests. For example, tests can be configured to stop as soon as a flaw is found or to look for all flaws. This helps to quickly determine if the site will fail compliance without performing the more exhaustive and time-consuming application tests. This "low hanging fruit" approach helps organizations to quickly determine if they have issues that must be addressed before more intensive tests are run or costly external auditors conduct a review.

Nessus also provides special features for web mirroring, allowing the user to specify which part of the web site will be crawled or excluded. The duration of the crawl process can be limited as well.

TENABLE AND MA 201 CMR 17

17.03: **Duty to Protect and Standards for Protecting Personal Information**
17.04: **Computer System Security Requirements**

Tenable's solutions can help with compliance by directly addressing a number of requirements in both of these sections.

Note: This section is based on the content of Massachusetts 201 CMR 17. Specific requirements are labeled and quoted directly from this law. How Tenable can help meet these requirements is also specified.

The following acronyms will be used:

- SC – SecurityCenter
- LCE – Log Correlation Engine
- PVS – Passive Vulnerability Scanner

17.03: Duty to Protect and Standards for Protecting Personal Information	How Tenable Can Help
(2)(b)2. employee compliance with policies and procedures; and (2)(b)3. means for detecting and preventing security system failures.	Nessus' compliance checks can be used to audit user accounts, specific lists of users as well as authentication and logging methods. The LCE normalizes all logs based on the user ID of the authenticated user. This allows quick and accurate inspection of all logs to determine which users have accessed systems with sensitive data. The LCE can also be configured with a list of all valid user accounts that access a particular asset group. When logins occur (failed or successful) the LCE can alert if the user in question is not on the authorized list. SC can manage multiple LCEs and provides powerful log search capabilities across multiple LCE instances. This facilitates an enterprise-wide search of a particular user's activity. SC can gather all of this information through the use of one or more LCEs. By analyzing historical attacks and anomalies detected in regular logs, network IDS tools and correlation with virus outbreaks, any organization can build a profile of their threats.
(2)(e) Preventing terminated employees from accessing records containing personal information.	Nessus can be used to audit if specific user accounts exist on various types of servers. The LCE can also be used to provide a list of all logs pertaining to deactivated and deleted user accounts. Multiple LCEs can be leveraged and managed by a central SC to monitor this activity across the enterprise. The LCE can also produce lists of users that have logged into various servers and specifically highlight events where login-failures were the results of deactivated accounts.
(2)(f)2. Requiring such third-party service providers by contract to	The PVS can be used to gain information about third parties without actually scanning them.

implement and maintain such appropriate security measures for personal information	Vulnerability and compliance information can be gathered to SC with just a few PVS installations. Nessus scanners with the ProfessionalFeed can also be used to perform a scan of these vendors to see if there are any potential compliance issues.
(2)(h) Regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrading information safeguards as necessary to limit risks.	Tenable's Unified Security Monitoring solution, which combines log analysis, anomaly detection, network scanning, patch auditing, configuration auditing and passive network monitoring, places a great deal of compliance reporting and monitoring data at your fingertips. SC and the LCE allow any organization to implement their compliance monitoring policy in real-time. These events are also available for reporting and historical records.
(2)(j) Documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.	SC can be used as a communications platform for incident response, vulnerability management and compliance monitoring solutions. SC provides the ability to save all LCE data from a suspected incident in a separate report along with a checksum that aids in the analysis phase of incident response.
17.04: Computer System Security Requirements	**How Tenable Can Help**
(1) Secure user authentication protocols including: (a) control of user IDs and other identifiers; (b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices; (c) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect; (d) restricting access to active users and active user accounts only; and (e) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on	Any system that logs user activity by user name also produces access control (login and login failures) logs. These can be used for log analysis, raw pattern searches and anomaly detection by the LCE. The LCE also provides the ability to associate an IP address with a user name and log if a user changes IP addresses. SC can be used to regularly scan for default user accounts and to search the full log data from multiple LCEs, providing an enterprise-wide view of user activity. The LCE can also be configured with a list of all valid user accounts that access a particular asset group. When logins occur (failed or successful) the LCE can alert if the user in question is not on the authorized list. The LCE can be used to provide a list of all logs pertaining to deactivated and deleted user accounts. Multiple LCEs can be leveraged and managed by a central SC to monitor this activity

access for the particular system; (2) Secure access control measures that: (a) restrict access to records and files containing personal information to those who need such information to perform their job duties; and (b) assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls	across the enterprise. This facilitates and enterprise-wide search of a particular user's activity. The LCE can also produce lists of users that have logged into various servers and specifically highlight events where login-failures were the results of deactivated accounts. The LCE normalizes all logs based on the user ID of the authenticated user. This allows quick and accurate inspection of all logs to determine which users have accessed systems with sensitive data.
(3)Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.	Nessus can be used to recognize the supported protocols that enable encrypted communications. Nessus actively tests all SSL systems, including wireless systems, for compliance with industry-recognized standards. This includes verification of host names that keys are tied to and testing the age of the SSL library to ensure that it is up to date. SC and PVS can be configured to test for several items including the presence of encryption software, the detection of an email sent that has been scripted by the software and emails sent that contain credit card data that was not encrypted. The LCE can also be used to log system events form network devices such as WiFi appliances, NAT firewalls and other hardware. The full log search capability provided in SC and LCE can be used to easily search and monitor all logged wireless data across the enterprise.
(4) Reasonable monitoring of systems, for unauthorized use of or access to personal information	Tenable's Unified Security Monitoring solution, which combines log analysis, anomaly detection, network scanning, patch auditing, configuration auditing and passive network monitoring, places a great deal of compliance reporting and monitoring data at your fingertips.
(6) For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information.	SC and the PVS can monitor any enterprise to determine connectivity between various points on the network. This helps ensure an appropriate firewall policy is in place and can help detect unauthorized changes. The LCE can also alert and report when changes to devices such as firewalls have occurred. SC can be used to search the full log data from multiple LCEs, providing an

	enterprise-wide view of logged activity. The 3D Tool can be used to display the locations of firewalls within the network. Nessus and the PVS have various methods to detect firewalls as well. SC and Nessus can be used to perform patch audits of Unix, Windows and router devices. This audit can occur across a sampling of the network, or all of it. Patch auditing is highly accurate and has a very low false positive and false negative rate because it uses file-based analysis to ensure that patches are deployed. Other techniques to assess patch deployment status such as examining the registry do not perform a complete audit.
(7) Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.	SC, Nessus and the PVS can be used to discover installed anti-virus instances and determine if assets have been updated. Nessus can be used to audit systems for the presence of a standard anti-virus solution and to also test that the solution is configured and working properly. Nessus can also determine if a required reboot has taken effect to activate an anti-virus update.
(8) Education and training of employees on the proper use of the computer security system and the importance of personal information security.	By using Tenable's products for vulnerability assessment, compliance, IDS analysis and log analysis, IT staff will have to learn a less complex set of tools than from using multiple products from many different vendors. Tenable provides a variety of training options to fit diverse needs, including classroom, virtual classroom, on-demand and onsite training.

ABOUT TENABLE NETWORK SECURITY

Tenable Network Security, the leader in Unified Security Monitoring, is the source of the Nessus vulnerability scanner and the creator of enterprise-class, agentless solutions for the continuous monitoring of vulnerabilities, configuration weaknesses, data leakage, log management and compromise detection to help ensure network security and FDCC, FISMA, SANS CAG and PCI compliance. Tenable's award-winning products are utilized by many Global 2000 organizations and Government agencies to proactively minimize network risk. For more information, please visit http://www.tenable.com.

Tenable Network Security, Inc.
7063 Columbia Gateway Drive
Suite 100
Columbia, MD 21046
410.872.0555
www.tenable.com