Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Defense in Depth: Employing a Layered Approach for Protecting Federal Government Information Systems

United States federal government agencies, whether civilian or military, are a regular target of cyber-attacks from a variety of sources. These sources range from amateur to experienced hackers, hostile nation states, or even agency personnel. Agency information systems are good targets for cyber-criminals because their information systems hold a treasure trove of data. The data is not only about their employees, but private citizens as well. Unlike private sector corporations, government agencies have to comply with s...

Copyright SANS Institute
Author Retains Full Rights

AD

Defense in depth: Employing a layered approach for protecting federal government information systems

GIAC GSEC Gold Certification

Author: Stacy Jordan, stacyj@tmo.blackberry.net
Advisor: Rick Wanner

Accepted: November 16th, 2012

Abstract

United States federal government agencies, whether civilian or military, are a regular target of cyber-attacks from a variety of sources. These sources range from amateur to experienced hackers, hostile nation states, or even agency personnel. Agency information systems are good targets for cyber-criminals because their information systems hold a treasure trove of data. The data is not only about their employees, but private citizens as well. Unlike private sector corporations, government agencies have to comply with specific legal statues and regulations from Congress and oversight bodies that govern their information systems. Additionally, agencies are required to disclose some of their data to the general public over the Internet. With this in mind, agencies have to ensure their most sensitive information is not improperly disclosure. A poor information security posture can put spies and military troops in harm's way and expose private citizens to cybercrime as well. Federal agencies need to employ a layered approach to information security in order to defend their systems from all threat sources. This paper will provide information on specific techniques that are being used by a major federal agency to protect their enterprise from threats.

© 2012 The SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

1. Introduction

When the Internet was invented in the late 1960's to conduct research between specific colleges and the US Department of Defense (DOD), no one envisioned that in the future networks would be connected into a singular global one. Prior to the 1980's, computers were too expensive to purchase for small business and home use. Once the MS-DOS operating system could be used by other computer manufacturers, "they began producing personal computers that were called PC-clones or IBM compatibles." (Techterms, 2011). Because of PC-cloning, the cost of manufacturing and purchasing, a computer decreased dramatically and this allowed computers to replace typewriters as the primary business tool.

[Today,] "we live an information age. Companies that are successful are those that are able to harness and utilize information to their competitive advantage. Along the same lines, economies and countries that are successful in this age are the ones that are networked; information based and those who empower their population" (Dontamsetti & Narayanan, 2009). As computer technology has advanced, agencies have become very dependent on computerized information systems to carry out their operations and to process, maintain and report essential information. "Virtually all US federal operations are supported by automated systems and electronic data; agencies would find it difficult if not impossible to carry out their missions without these information assets" (GAO, 2010). As a result, federal agencies have to safeguard their information assets in a way to prevent harm.

1.1. Key terms defined

Before discussing techniques that US federal governments can use in developing a defense-in depth strategy, it is necessary to define a few key terms. Information security defined by 44 U.S.C Section 3542 is "the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destructions in order to provide confidentially, integrity and availability (CIA)" (Kissel, 2010). CIA is very relevant to agencies because their data should be protected based on ensuring privacy, authenticity, and reliability. A term that is used interchangely with information security is computer security. "Computer security protects your computer and everything associated with it-[including] your building, your terminal and printers, your cabling and your disk and tapes" (Russell and Gangemi, 1991). Computer

© 2012 The SANS Institute Author retains full rights.

or information security has evolved over the past two decades. Right now, we are in the third generation (3G) and the focus has changed from being technology focused to process focused. "The shift in focus from technology to processes, and subsequently the human element, has come with the realization that technology and processes are only as good as the human beings that use them" (Dontamsettin & Narayanan, 2009). Humans, specifically agency personnel are a high threat to security and later in this paper the subject of internal threats will be discussed.

Even though information security has evolved, the goal of information security has not changed, "the main [goal] of information security is to sustain and defend three critical security properties: confidentiality, availability and integrity" (Dontamsettin & Narayanan, 2009). US government information systems are categorized based on their confidentiality, integrity and availability as defined by National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS 199). This comes into play during the authorization and accreditation process (A&A) formally known as certification and accreditation (C&A) (NIST, 2004). Depending on the data and system categorization, agencies can employee different techniques to protect both data and systems.

US federal civilian agencies and departments are strongly encouraged to use NIST standards for protecting their data and information systems. Agencies that deal with intelligence data use National Security Council (NSC) guidelines while the military implement standards from the Defense Information System Agency (DISA). All these agencies define defense in depth as establishing variable barriers across multiple layers and the intelligent applications of techniques and technologies that exist today. Defense in depth helps agencies protect network resources even if one of their security layers has been compromised. After all, "no single security component can be guaranteed to withstand every attack it might need to face" (Northcutt & Zeltser, 2006). You can look at defense-in-depth as protecting the threats that come from outside (perimeter) and inside (internal) which includes agency partners (contractors).

"Defense-in-depth is often described as an ‘onion,' whereas an intruder will have to go through many layers to get access to the important data of a specific company. Moreover, a combination of multiple layers will be more effective against unpredictable attacks than will be a single dense [one] optimized for a particular type of attack" (Vacca, 2009). Defense-in-depth allows an agency to see the attack in the early stages which will help decrease the likelihood of a data breach or major compromise. Civilian agencies not only have to utilize the latest technologies to protect their information systems but applicable federal laws as well.

© 2012 The SANS Institute Author retains full rights.

1.2 Laws governing information security and information systems with US civilian agencies

All US civilian government agencies are bound by legal statutes enacted by the US Congress and regulations from oversight agencies (e.g. General Accounting Office, NIST, and Office of Management and Budget) in the way information security and information systems are managed. Some of the regulations and statutes agencies must be compliant to include Special Publications (SP), Federal Information Processing Standards (FIPS), Freedom of Information Act (FOIA), the Privacy Act and E-Government Act of 2002 (PL 107-347). In addition, Congress enacted Public Law 109-461 (veterans' benefits, health care and information technology act of 2006) in response to the US Department of Veterans Affairs (VA) breach of approximately 26 million veteran's data.

The cause of the data breach was due to theft of an unencrypted laptop from an agency contractor's home. Even though the files on the laptop were never accessed and no apparent identity threat occurred, the VA had to pay a judgment of over 20 million dollars in January 2009. The VA CIO is required to submit both a monthly and quarterly reports to Congress detailing data breaches and security breaches. Also, the CIO has to testify quarterly to Congress as well (US House of Representatives, 2006). The most influential regulation or law that affects civilian agencies information security policy is PL 107-347 also known as Federal Information Security Management Act (FISMA).

FISMA is Title III of the E-Government Act of 2002 and this law requires all federal civilian agencies to develop and implement an agency wide information security program. This document has to contain information concerning "security requirements, policies, controls and risks to the agency" (Taylor, 2007). Prior to FISMA, agency information security was governed under Government Information Security Reform Act (GISRA) that allowed them to document their security posture via self-assessment and independent review by their agency Inspector General office. Since its inception, FISMA has had its critics because most saw it as a “paper pushing” exercise; not a law that would improve the security posture of an agency (Jackson, 2010).

To improve federal civilian agency security posture, the President of the United States created a new position within the Executive Office of the President (EOP) called Cybersecurity Coordinator and gave the Department of Homeland Security (DHS) increased responsibility for not only protecting intelligence community information but civilian agencies as well. As a result, Office of Management and Budget (OMB) issued a memo in June 2010 to outline and clarify duties and responsibilities concerning FISMA.

© 2012 The SANS Institute Author retains full rights.

OMB will primarily be responsible for the annual FISMA reporting to Congress but "DHS will exercise primary responsibility within the executive branch for the operational aspects of Federal agency cybersecurity with respect to the Federal information systems that fall within FISMA under 44 U.S.C. §3543." (Orszag & Schmidt, 2010) With DHS taking the lead concerning operational information security, their first task was to find a way to strengthen agency annual FISMA reporting.

Since 2010, agencies have been required to use a new automated tool called CyberScope for their annual FISMA reporting (Zients, Kundra and Schmidt, 2010). This new reporting tool is a direct result of a Whitehouse task-force initiated in September 2009 to add outcome-focused metrics for federal agencies. Agencies when reporting their annual FISMA compliance, have to use government accepted benchmarking, interview key officials responsible for information security and provide DHS access via a direct data-feed into their specific security management tool. An agency FISMA report is deemed incomplete or inaccurate if all elements have not been satisfied. FISMA was structured around a three year certification and accreditation (C&A) process but this may not be a good indication that agency information systems are protected from threats.

NIST SP 800-37 Revision 1, Guide for Applying the Risk Management Framework (RMF) to Federal Information Systems: A Security Life Cycle Approach was created to move the C&A process from a three-year cycle to continuous monitoring. "Information security continuous monitoring (ISCM) is defined as maintaining ongoing awareness of information security, vulnerabilities and threats to support organizational risk management decisions" (NIST, 2011). So that civilian agencies have the necessary guidance to properly implement ISCM, NIST in partnership with other organizations has created two other publications. In February 2011, NIST released a draft publication that was co-developed by DHS and it is called NIST Interagency Report (IR) 7756: CAESARS Framework Extension: An Enterprise Continuous Monitoring Technical Reference Architecture (NIST, 2011). A second draft was released for public comment in January 2012. Once the final document is published, it will provide agencies with the technical framework to better implement ISCM. NIST published SP 800-137: Information Security continuous monitoring in September 2011 and this was the third publication created on continuous monitoring. To assist information security professionals with implementing RMF, an on-line course was created in late 2011. Now that the focus has changed in terms of information systems accreditation, will this new approach protect agency information systems and data from the various threats present today?

© 2012 The SANS Institute Author retains full rights.

2. Threats to federal government information systems

US Government Accounting Office (GAO) in their report to the US House of Representatives committee on Homeland Security (GAO-10-834T) documented the various threats to federal information systems and cyber-based critical infrastructure. In their report, interviewed government officials stated their main concern was "attacks from individuals and groups with malicious intent such as criminals, terrorists and foreign nations" (GAO, 2010). Other sources of threats include information warfare, hackers, virus writers and disgruntled employees and contractors. These sources can be classified into two types of threats to information systems: internal and external.

Internal threats to information systems are mostly defined as either current or former personnel (employee or contractor) of the agency. These individuals have greater access to sensitive information and security weaknesses through their current or previous work experience. Additionally, an insider has established a trust relationship so the person may not be questioned if seen in an authorized location or asks for special network access. A term that is synonymous with internal threats is the malicious insider. "A malicious insider is a current or former employee, contractor or other business associate who:

> Has or had authorized access to an organization's network system or data;
> Intentionally exceeded or misused that access in a manner that
> Negatively affected the confidentiality, integrity or availability of the
> organization's information or information systems." (CERT, 2009).

Not only do insiders directly cause harm to their agency network but cybercriminals use internal employees as their attack vector for causing mayhem as well.

One of the most successful methods that use insiders to harm their computing environment is through social engineering. Social engineering is when an attacker convinces an individual to perform an action and provide information about their computing environment that is not public knowledge. The attacker will usually state they are an IT support personnel and ask the "victim" to perform "diagnostic" activities which can assist them in their attack. Social engineering can be considered an external threat because an "outsider" will usually execute the attack and gain the trust of internal employees as a means to obtain network information for future exploitation.

External threats can be defined as "any vulnerability which can be exploited to gain access to an environment from outside the [host] environment" (Scudder, 2010). So what is vulnerability and how does it play a role? Vulnerability can be viewed as an attacker using a weakness in the information system or security policy to their advantage.

© 2012 The SANS Institute Author retains full rights.

Examples of vulnerabilities include the lack of software patch management, cross site scripting (XSS), weak passwords or unnecessary ports open on the agency firewall. Attackers will use software tools along with social engineering to exploit a particular vulnerability in order to gain access to agency information.

Some other external threats to federal information system include espionage and spear-phishing. Espionage in the case of federal government information systems is not necessarily from private sector competitors but foreign states that are looking to damage information systems for political or economic gain. Attackers will not only target federal information systems but key contractors as well. For example, two defense contractors were the subject of cyber attacks that led to exposure of sensitive data of their military and civilian clients in 2011 (Sternstein, 2011). Cybercriminals realize that attacking government contractors is a good way to reach their ultimate target since federal agencies have increased their overall security posture while contractors may be slow in adopting the same standards. A new and creative way for attackers to affect government information systems is by conducting a spear-phishing attack.

Spear-phishing is typically done via electronic mail (email) and it is specially crafted in order to gain unauthorized access to confidential data held by the agency. Examples of a successful spear-phishing attack email subject line include "mailbox exceeded," "helpdesk assistance required" or "password expired" that look like the message came from the agency system administrator. When the employee clicks on the link supplied in the message, they are asked for some type of confidential information (e.g. username and password). Because the message appeared from a trusted source, the employee(s) provide the requested information to the attacker on the bogus website. The attacker uses the victim's confidential information for network login and sends the same email message to personnel located in the victim's contact list. This allows the attacker to harvest more network credentials and increase the pool of people that have been compromised. Sometimes, attackers will use a fake social media website to obtain the same information as well. Whether or not the threat source is internal or external, the key focus of security is managing risk.

Risk management can be defined as "the process of managing risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system" (Kissel, 2011). With the change of C&A into a risk management framework (RMF) through the publication of NIST 800-37, all personnel who are responsible for information security have to ensure their data and systems are protected from threat sources that will utilize various tools to exposure agency risks. Examples of risks to information system include:"

© 2012 The SANS Institute Author retains full rights.

Resources, such as federal payments and collections, could be lost or stolen
Sensitive information, such as national security information, taxpayer data, social security records, medical records and proprietary business information could be inappropriate access and used for identity theft or espionage
Agency missions could be undermined by embarrassing incidents that results in diminished confidence in the ability of federal organizations to conduct operations and fulfill their responsibilities" (GAO, 2010).

Agency security professionals not only have to worry about the risk of agency data being exploited on their "protected" environment but outside as well due to recent presidential mandates. As a result of bad weather in 2009-2010, Office of Personnel Management (OPM) was charged by the president to increase the number of employees who have the ability to conduct official business in alternate work-site location.

Congress passed H.R. 1722-The Telework Enhancement Act of 2010 which "requires heads of agencies to establish and implement telework" (US House of Representatives, 2010). For the most part, agency employees or contractor will select their residence as their alternate work-site and they may even use their personal computing devices (e.g. Apple Ipad, Android Tables, etc.) Since these devices are primarily consumer focused, they may not have undergone rigorous security testing to support their usage in government. As IT budgets are decreased across government due to mandatory cuts, agency and department CIOs have to use creative ways to stretch their budget.

With personal IT devices being used for telework, CIOs are developing security policies and procedures for personnel to bring their own device (BYOD) into the workplace. BYOD will allow agency personnel to use their personal device as long as they agree to specific security requirements. In August 2012, Federal CIO Council along with the Digital Services Advisory Group released a "BYOD toolkit" which provides agency CIOs with case studies and policy examples that can be leverage in creating their own policy (US Federal CIO Council, 2012). Security professionals now need to weight the business case for using personal devices and their lack of security in a new light.

In addition, the president also mandated executive agencies and departments to start using cloud computing for data and information services through the "Cloud First" initiative. An agency is compliant by using one of the three types of cloud computing: Infrastructure as a Service (IaaS), Software as a Service (SaaS) and Platform as a Service (PaaS). The premise behind using cloud computing is to eliminate the need for agencies and departments to have their own data centers for application hosting and storage.

© 2012 The SANS Institute Author retains full rights.

Instead, agencies are to rely on certified third-party vendors to host agency data and applications. Currently, a few agencies are using private cloud service providers to comply with this new mandate while others are building their own agency cloud environment. With these new changes occurring, how can agency security professionals keep their data and information systems secure when they are located all over the place?

3. Defense in depth illustrated: techniques for protecting federal information systems

Regardless of the type of organization (private sector or government), using defense-in-depth to secure your data and information system is a good strategy. Defense-in-depth allows an organization to build their security posture based on best practices in the hardware, software and policy arena. Hardware protection devices include firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), host intrusion protection system (HIPS) and biometric devices (e.g. retinal scanning, secure token devices, etc.). Software based protection include anti-virus software, automated patch management, Internet monitoring software and computer port blocking software. Good information security policy contains requirements for agency personnel to comply with security awareness training requirements, security incident reporting and accreditation of information systems.

Even with these mechanisms in place to protect data and information systems from malicious activities, the end user (human factor) can derail those measures by not following proper procedures. In this section of the paper, information will be provided on how a major federal agency utilized hardware, software and policy to keep its data and information system protected.

3.1 Hardware protection

One of the first protective measures implemented by this agency was portable media encryption. Hard disk encryption is mandatory for laptops and desktops located in "hoteling sites." Hard disk encryption is a good way to ensure that sensitive data stored on desktop and laptop computers are protected. Software is employed to encrypt the whole disk and the end-user must enter valid credentials to “access” the drive. Two different applications are used at this agency depending on the operating system of the equipment. Symantec End-point Encryption (SEE) is used for Windows based operating system and Pretty Good Privacy (PGP) for Apple laptops. SEE requires that the device (desktop or laptop) "check-in" to the master server every 90 days. In the event that the

© 2012 The SANS Institute Author retains full rights.

device does not check-in within the required time-frame, the end-user is locked-out of the local device and has to call local IT support for assistance. PGP does not require the Apple laptop to "check-in" to the network but it does enforce network password management. Not only is hard disk encryption in use but the agency is utilizing personal identity verification (PIV) card encryption for email as well. PIV card encryption requires smartcard access and personnel either have a reader physically attached to their equipment or using agency provided USB device.

The agency also requires all system administrators to utilize two factor authentication when performing administrative tasks. System administrator has to use a USB token to complete tasks that require elevated privileges. The use of two-factor authentication will prevent hackers who obtained the userid/password a system administrator from doing any harm. The agency deploys other hardware protective devices at its gateways to help with data lost prevention and web-content filtering. To ensure agency personnel cannot send sensitive information, specifically social security numbers (SSNs) via unencrypted email, all agency email goes through an Iron Port appliance.

This appliance checks the complete email including attachments for numbers that resemble SSNs and blocks the email if it was not sent using encryption. In the event that the message was blocked in error, the employee must send the network security operations center (NSOC) an email which contains the block information so the message can be reviewed. Web-content filtering is performed using Palo Alto Network's next generation firewall. This equipment prevents agency personnel from visiting certain sites that have been classified as either malicious or contains inappropriate content (e.g. alcohol, gambling, streaming audio). The firewall will even block the site when it is set-up using hyper-text transfer protocol over secure-socket layer (HTTPS). Finally, the agency uses IDS and IPS that are centrally managed by the NSOC. NSOC is staffed 24/7 so it can response at a moment's notice to potential attacks.

3.2. Software protection

In terms of software protection deployed by the agency, it uses Mcafee E-Policy Orchestrator (ePo) and associated products on all Windows based equipment. Apple products currently do not have an enterprise anti-virus solution but suspicious traffic is registered. All agency equipment is registered with the master ePo server and information security officers (ISOs) receive an email when a device is suspected with some type of malicious software. Patch management for all Windows based equipment

© 2012 The SANS Institute Author retains full rights.

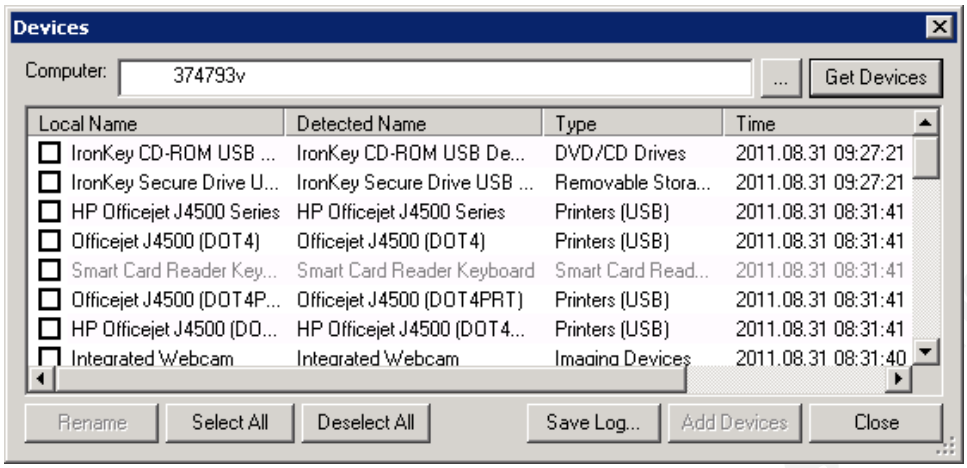
is done through a combination of Microsoft System Center Configuration Management (SCCM) and IBM's Tivoli Endpoint Manager (BigFix). SCCM is used on all equipment that is directly connected to the agency network and is configured to execute the required monthly Microsoft patches during off-peak hours. BigFix product is used to provide smaller system patches to remote connected computers and visibility to agency assets to management. BigFix is set-up to run a report on specific items of interest across a specified network domain or enterprise-wide. Items of interest include operation system vulnerability, encryption software version, device model and operating system. The system can be configured to run different dashboards to show compliance level and data can be exported as a comma separated value (CSV) file or printed.

The agency uses software public key infrastructure (PKI) to protect email messages that contain sensitive data. Agency personnel and partners can obtain certificates in order to properly secure messages that contain information like social security number, medical conditions, bank account number or employee performance ratings. Alternate software method for protecting email is through Microsoft Right Management Services (RMS) and this allows the sender to restrict properties of the email (e.g. printing, copying and forwarding). RMS only works with internal agency users and sending sensitive data outside of the agency environment requires the use of encryption.

Other software protective measures used deal with forensics and port blocking. All Windows based computing devices have Encase forensic software applet installed. This allows NSOC personnel to conduct initial forensic investigation “over the wire” as a means to catch potential compromise in real time. In the event that the “over the wire” forensic did not work, IT support will remove the drive and send to NSOC using proper chain of custody procedure. If a serious infection has occurred, NSOC personnel will make contact with the ISO in order to have the machine taken off-line.

To protect agency data from being lost via removable devices, software has been deployed to all agency computer equipment to restrict use of CD/DVD drive and USB ports. The software is called Sanctuary and it is a product of Lumesion and it prevents agency personnel from writing to CD/DVD drive or portable media connected to USB port without their computer being added to a "white-list." ISOs submit a request for the computer to be placed on the "white-list" which will allow access to use either CD/DVD drive or USB port. In some cases, the agency employee will have the ability to write CD/DVD drive and USB port. Below is what a sanctuary administrator will see when verifying a workstation can access the appropriate device or port.

© 2012 The SANS Institute Author retains full rights.



3.3. Policy

Over the past three years, information security policy at this agency has grown to cover how personnel are trained on their information security responsibility and ensuring contracts have the appropriate information security language. Most of these policies are integrated into the duties of ISOs but IT personnel, contracting officers (COs) and supervisors play a role in compliance as well. Agency use software protective measures to enforce agency-wide security policies (e.g. prohibited use of non-encrypted and non-agency issued flash drives, using bandwidth intensive applications, downloading unauthorized software) as a means to decrease exposure to malicious software. All agency employees, volunteers and contractors are required to take security awareness training and privacy training within 30 days of on-boarding (entry into duty). Mandatory training is conducted through the agency's talent management system (TMS) but in some cases training can be done through a security presentation conducted by the facility ISO or privacy officer (PO).

Security training provides information on what should be done in certain situations (e.g. sensitive information protection, virus attack or lost or stolen equipment). Medical personnel and trainees have to take specialized Health Insurance Portability and Accountability Act (HIPAA) training as a division of the agency is a covered entity for the purpose of HIPAA. This additional training provides information on how to protect medical information so it is not subject to a data breach. Refresh training is required on a yearly basis and all divisions within the agency need to be 98% compliant on training. In the event that agency personnel do not take required training in the prescribed time-frame, access to information system will be denied or removed (if applicable).

Another policy to improve information security posture is to ensure all employees with significant information security responsibility complete role-based training. This

© 2012 The SANS Institute Author retains full rights.

training has to be completed within 60 days of the individual being assigned to the position. Depending on the role, the individual may take one course which is tailored to their specific job (e.g. database administrator, system administrator, CIO, etc.). In the event that a possible information security event occurs at the agency, policy requires reporting within one hour of the event to either a facility ISO or NSOC personnel. Types of reportable events include lost or stolen government furnished equipment (e.g. Smartphone, broadband card, and laptop), lost identification badge or virus.

Agency ISO and PO personnel use a ticketing system to report potential information security or privacy incidents to NOSC. NOSC personnel conduct initial triage and verify ISO or PO report is truly classified as a security incident. Also, potential incidents are checked for possible data breach via data breach response team (DBRT). This team ensures that all necessary reporting procedures are followed if a breach has been confirmed. Incidents that involve malicious code require verification that equipment has been appropriately remediated (e.g. anti-virus scan, re-imaging or application patching). Because the agency deals with medical devices, incidents that affect this type of equipment are tracked and require special remediation from the equipment vendor. Daily incidents are submitted to DHS through their Computer Emergency Response team (US-CERT).

The agency has also established a policy concerning the use of a standardized security clause for all contracts. This clause requires vendors who win IT contracts to adhere to agency and federal government policy and regulations concerning information system accreditation. All third-party vendors who host, process, transmit and store agency sensitive information are required to be accredited and their documentation must be supplied to their contracting official representative (COR) and turned over to the facility ISO for review. ISO will consult certification program office to ensure that supplied documentation meets current standards. Also, any IT contract that will be using a cloud service provider (CSP) has to ensure that vendor has started the cloud computing assessment process through GSA called Federal Risk and Authorization Management Program (FedRamp) (GSA, 2012).

FedRamp is similar to FISMA but addresses special security concerns that cloud computing presents and is required by agencies for low and moderate rated information systems. GSA has published the first set of third party assessment organizations that can be used by CSP to obtain FedRamp authorization. CSPs have to maintain their security posture through continuous monitoring and their authorization may not be for a three year period. The security clause allows the agency to verify contractor security posture through inspector general FISMA audits and/or FISMA annual assessment process. At

© 2012 The SANS Institute Author retains full rights.

the end of the contract, the vendor has to destroy all associated media using approved methods outlined in NIST SP 800-88: Guidelines for media sanitization.

4. Conclusion

US federal government agencies have a huge amount of data that they are required to collect and protect. This data is stored and processed in multiple information systems that are subject to cyber-attack from various sources. Threat sources range from hackers to foreign states and even disgruntled employees. Information security professionals along with agency CIOs have a challenge defending their agency because some of their systems and data reside in other locations. Agencies have to perform due diligence and ensure their vendors have undergone the proper accreditation especially if they are utilizing cloud computing technology.

In addition, telework and budget cuts have incorporated personal computing devices into the agency computing arena as well. These new devices add new risks due to their lack of full security testing for government use. In light of all these hurdles, what is the best strategy to protect government information systems and data? Utilizing defense-in-depth is an appropriate strategy in a variety of ways. It helps security professionals use best practices concerning hardware and software protective measures and eliminate the possibility for a single point of failure. Also, agency CIOs can establish policies and procedures that all personnel need to follow as a means of minimizing risk. The key to protecting US federal government information systems is ensuring that all components used in the defense-in-depth approach are current. Without proper compliance, it does not matter what tools or procedures are in place as the action of one individual can cause great harm to the agency.

Stacy Jordan, stacyj@tmo.blackberry.net

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

5.0 References

B., Jon. and Scudder, R. (editor) (2010, December 9). Questions in computer security: what is an external threat? Retrieved from http://www.sans.org/reading_room/whitepapers/bestprac/guide-government-security-mandates_1000

IBM Compatible. *Techterms*. Retrieved January 12, 2011, from http://www.techterms.com/definition/ibmcompatible

Jackson, W. (2010, April 26). *FISMA gets the tools to do the job*. Retrieved from http://gcn.com/articles/2010/04/26/cybereye-fisma-best-practices.aspx

Kissel, R. US Department of Commerce, NIST. (2010). *Draft glossary of key information security terms* (NIST IR 7298(Draft)). Retrieved from http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf

Northcutt, S, & Zeltser, L. (2005). I*nside network perimeter security*. Indianapolis, IN: Sams

Orszag, P, & Schmidt, H. Executive Office of the President, Office of Management and Budget. (2010). *Clarifying cybersecurity responsibilities and activities of the Executive Office of the President and the Department of Homeland Security* (M-10-28). Washington, DC: Retrieved from http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-28.pdf

Russell, D, & Gangemi, G.T. (1995). *Computer security basics*. O'Reilly.

Sternstein, A. (2011, May 29). DOD, DHS jointly respond to military contractor cyber attack. *NextGov*. Retrieved from http://www.nextgov.com/technology-news/tech-insider/2011/05/dod-dhs-jointly-respond-to-military-contractor-cyber-attack/54570/

Taylor, L. (2007). FISMA certification & accreditation handbook. Rockland, MA: Syngress

© 2012 The SANS Institute Author retains full rights.

U.S. Department of Commerce, National Institute of Standards and Technology. (2011). *Caesars framework extension: an enterprise continuous monitoring technical reference architecture (draft)* (NIST Interagency Report 7756 (Draft)). Gaithersburg, MD: Retrieved from http://csrc.nist.gov/publications/PubsDrafts.html#NIST-IR-7756

U.S. Department of Commerce, National Institute of Standards and Technology. (2004). *Standards for security categorization of federal information and information systems*. Retrieved from website: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

US Federal CIO Council. (2012, August). *Bring your own device: A toolkit to support federal agencies implementing*. Retrieved from https://cio.gov/wp-content/uploads/downloads/2012/09/byod-toolkit.pdf

US General Services Administration. (2012, June 29). *Fedramp faqs.* Retrieved from http://www.gsa.gov/portal/category/102439

U.S. Government Accountability Office, (2010). *Cybersecurity: continued attention is needed to protect federal information systems from evolving threats (GAO-10-834T)*. Washington, DC: Retrieved from http://www.gao.gov/new.items/d10834t.pdf

U.S. House of Representatives and U.S. Senate (2006, December 22). *Public law 109–461*. Retrieved from http://www.gpo.gov/fdsys/pkg/PLAW-109publ461/pdf/PLAW-109publ461.pdf

US House of Representatives. (2010, January 5). *H.R. 1722*. Retrieved from http://www.gpo.gov/fdsys/pkg/BILLS-111hr1722enr/pdf/BILLS-111hr1722enr.pdf

Vacca, J. (2009). *Computer and information security handbook*. Burlington, MA: Morgan Kaufman.

Zients, J, Kundra, V & Schmidt, H. Executive Office of the President, Office of Management and Budget. (2010). *FY 2010 reporting instructions for the federal*

© 2012 The SANS Institute Author retains full rights.

information security management act and agency privacy management (M-10-15). Washington, DC: Retrieved from http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-15.pdf

© 2012 SANS Institute, Author retains full rights.

Stacy Jordan, stacyj@tmo.blackberry.net

© 2012 The SANS Institute Author retains full rights.

Appendix A:

Listing of federal government laws and procedures governing cybersecurity

Government paperwork reduction act:
http://www.whitehouse.gov/omb/fedreg_gpea2/
Freedom of Information Act (FOIA):
http://www.justice.gov/oip/foia_updates/Vol_XVII_4/page2.htm
Federal Information Security Management Act(FISMA):
http://csrc.nist.gov/drivers/documents/FISMA-final.pdf
Privacy Act of 1974: http://www.usdoj.gov/opcl/privacyact1974.htm
FedRAMP: http://www.gsa.gov/portal/category/102375
Computer Security Act of 1987: http://www.nist.gov/cfo/legislation/Public%20Law%20100-235.pdf
Office of Management and Budget memoranda:
http://www.whitehouse.gov/omb/memoranda_default
NIST Special Publications: http://csrc.nist.gov/publications/PubsSPs.html
NIST FIPS publications: http://csrc.nist.gov/publications/PubsFIPS.html
Open Government Act of 2007:
http://www.justice.gov/oip/amendment-s2488.pdf

Links to US federal government cybersecurity policies and standards

United States Department of Homeland Security, Federal Network Security
http://www.dhs.gov/files/programs/federal_network_security.shtm

United States Chief Information Officer (CIO) council security & privacy:
http://www.cio.gov/module.cfm/node/priorities/psec/3

United States Computer Emergency Response Team:

http://www.us-cert.gov/reading_room/

Stacy Jordan, stacyj@tmo.blackberry.net

© 2012 The SANS Institute Author retains full rights.

Appendix B:

Product vendors' web-site links

Lumension (Sanctuary port blocking software):
http://www.lumension.com/device-control-software/

Whitepaper on SCCM and Sanctuary:
http://www.lumension.com/Products/device-control-software/lumension-device-control-for-system-center.aspx

Microsoft System Control Configuration Manager (SCCM):
http://www.microsoft.com/systemcenter/en/us/configuration-manager/cm-overview.aspx

Encase Forensic software:
http://www.guidancesoftware.com/resources-brochures.htm

PGP whole disk encryption:
http://www.symantec.com/business/whole-disk-encryption

BigFix Enterprise Suite (acquired by IBM):
http://www-01.ibm.com/software/tivoli/solutions/endpoint/?s_pkg=bfwm

Mcafee E-policy orchestrator (ePo):
www.mcafee.com/us/products/epolicy-orchestrator.aspx

Guardian Edge (acquired by Symantec):
http://www.guardianedge.com/resources/guardianedge-hard-disk-encryption-faq.php

Stacy Jordan, stacyj@tmo.blackberry.net

© 2012 SANS Institute, Author retains full rights.

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**