Department of Homeland Security
Office of Inspector General

DHS Needs to Improve the Security Posture of Its Cybersecurity Program Systems

OIG-10-111

August 2010

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 25028

Homeland Security

AUG 18 2010

Preface

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the department.

This report addresses whether physical and logical access controls are in place to secure the cybersecurity program systems utilized by the National Cyber Security Division and to ensure the integrity and reliability of the information it disseminates to the public and private sectors. It is based on interviews with key management officials, as well as system and contractor personnel, physical security evaluations, system security vulnerability assessments, and reviews of applicable documentation.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. We trust this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

Frank W. Deffer
Assistant Inspector General, IT Audits

Table of Contents/Abbreviations

Appendices

Abbreviations

C&A	Certification and Accreditation
CNCI	Comprehensive National Cybersecurity Initiative
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GAO	Government Accountability Office
HSIN	Homeland Security Information Network
IA	Information Assurance
IP	Internet Protocol
ISA	Interconnection Security Agreement
IT	Information Technology

MOE	Mission Operating Environment
MOU/A	Memorandum of Understanding/Agreement
NCPS	National Cybersecurity Protection System
NCSD	National Cyber Security Division
NIST	National Institute of Standards and Technology
NPPD	National Protection and Programs Directorate
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
SBCG	Secure Baseline Configuration Guide
SOP	Standard Operating Procedure
SP	Special Publication
SSP	System Security Plan
ST&E	Security Test and Evaluation
STIG	Security Technical Implementation Guide
TAF	Trusted Agent FISMA
TIC	Trusted Internet Connection
US-CERT	United States Computer Emergency Readiness Team

Executive Summary

Cyber threats pose a significant risk to economic and national security. In response to these threats, the President, legislators, experts, and others have characterized cybersecurity, or measures taken to protect a computer or computer system against unauthorized access or attack, as a pressing national security issue. The National Cyber Security Division (NCSD) was established to serve as the national focal point for addressing cybersecurity issues in the public and private sectors.

The United States Computer Emergency Readiness Team (US-CERT), created under NCSD, is responsible for compiling and analyzing information about cybersecurity incidents and providing timely technical assistance to operators of agency information systems regarding security incidents. The team provides response support and defense against cyber attacks for the federal civil executive branch (.gov); disseminates reasoned and actionable cybersecurity information to the public; and facilitates information sharing with state and local government, industry, and international partners.

Our audit focused on the security of the systems that US-CERT uses to accomplish its cybersecurity mission. Overall, NCSD has implemented adequate physical security and logical access controls over the cybersecurity program systems used to collect, process, and disseminate cyber threat and warning information to the public and private sectors. However, a significant effort is needed to address existing security issues in order to implement a robust program that will enhance the cybersecurity posture of the federal government. To ensure the confidentiality, integrity, and availability of its cybersecurity information, NCSD needs to focus on deploying timely system security patches to mitigate risks to its cybersecurity program systems, finalizing system security documentation, and ensuring adherence to departmental security policies and procedures.

We are making 10 recommendations to the Director, NCSD. NCSD has already begun to take the actions to implement them. National Protection and Programs Directorate (NPPD)'s response is summarized and evaluated in the body of this report and included, in its entirety, as Appendix B.

Background

The Department of Homeland Security (DHS) is responsible for leading the protection and defense of federal civil executive branch networks against cyber threats, and coordinating response to cyber attacks and security vulnerabilities. To secure the Nation's cyberspace and assets, DHS established NCSD in June 2003. NCSD, which operates within NPPD, is the national focal point for cybersecurity in the public and private sectors. NCSD addresses threats to federal government systems and takes the lead in instituting the objectives of the Comprehensive National Cybersecurity Initiative (CNCI).[1] This initiative authorizes DHS, together with the Office of Management and Budget (OMB), to establish minimum operational standards for federal civil executive branch networks so that US-CERT can direct the operation and defense of government connections to the internet.

Created in September 2003, US-CERT, one of NCSD's branches, is charged with protecting the Nation's information infrastructure by coordinating defense against and response to cyber attacks. US-CERT analyzes data to reduce security threats and vulnerabilities, disseminates cyber threat warning information to promote public awareness of the threats, and coordinates incident response activities. US-CERT utilizes four main information systems to help accomplish its mission:

- Mission Operating Environment (MOE).
- National Cybersecurity Protection System (NCPS) (known operationally as Einstein).
- Homeland Security Information Network (HSIN)/US-CERT Portal.
- NCPS Public Web (www.us-cert.gov).

The MOE is the backbone of US-CERT operations. It provides a basic computing environment that allows US-CERT personnel to exchange and access mission-critical security incident data and information system anomalies. The MOE is a secure and stabilized network infrastructure that supports US-CERT program operations, such as email and user access to NCPS Einstein data.

[1] Formalized in January 2008, the CNCI established a multipronged approach for the federal government to identify current and emerging cyber threats and respond to or proactively address state and non-state adversaries targeting information systems and infrastructure for exploitation and potential disruption or destruction.

Through the NCPS program, US-CERT has established an automated process for collecting, correlating, analyzing, and sharing potential threats and security information across the federal government to improve our Nation's situational awareness of cybersecurity. In its current state, NCPS Einstein incorporates network intrusion detection technology to help defend federal executive agency information technology (IT) enterprises from potential security attacks.[2] NCPS Einstein enables US-CERT to gain increased knowledge of federal executive agency networks and fulfill its mandate to act as a central point of responsibility for improving the network security of the federal government.

In November 2007, OMB announced the Trusted Internet Connection (TIC) initiative, which is intended to improve the federal government's security posture by reducing the number of external internet connections used by the government.[3] The TIC initiative aims to reduce and consolidate the number of external connections to create a more clearly defined "cyber border," and allow for fewer external connections that can potentially be used for malicious attacks. In response to the TIC initiative, Einstein sensors are currently being deployed at the reduced number of internet gateways to more effectively monitor network activity across the federal government. With the exception of the Department of Defense, federal agencies' participation in NCSD's Einstein program became mandatory with the implementation of the TIC initiative.

There are currently two versions of NCPS Einstein, known as Einstein 1 and Einstein 2.[4] Einstein 1 sensors collect network flow information and provide a high-level perspective from which to observe potential malicious activity in the computer network traffic of participating agencies' networks. The network flow data collected by Einstein sensors is aggregated from all participating departments and agencies, then analyzed to detect network anomalies spanning the federal government. The network flow data collected consists of the following information:

[2] Network intrusion detection technology automates the intrusion detection process. Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for possible violations or the imminent threat of violations of computer security policies, acceptable use policies, or standard security practices.

[3] OMB Memorandum M-08-05, *Implementation of Trusted Internet Connections (TIC)* (November 20, 2007).

[4] Development of Einstein 1 began in 2003; deployment began in March 2005. Development of Einstein 2 began in January 2008; deployment began in August 2008.

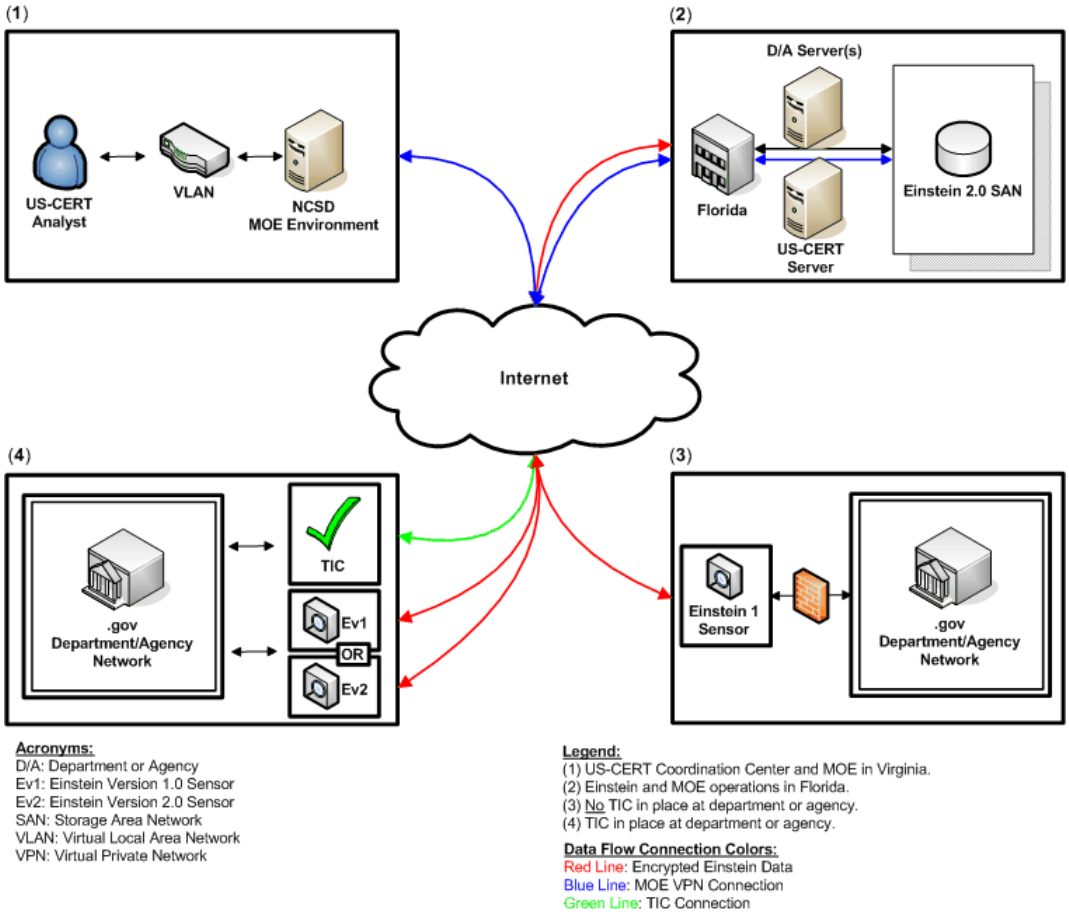
- Source internet protocol (IP) address of the computer that connects to the federal information system.
- Destination IP address.
- Port the connection was initiated on by the source computer.
- Port the connection was received on by the destination computer.
- Protocol used to transport the data.
- Start/end time of the communication.

Einstein 2, an updated version of Einstein 1, incorporates network intrusion detection technology capable of alerting US-CERT to the presence of malicious or potentially harmful computer network activity in federal executive department and agency network traffic. Einstein 2's network intrusion detection technology uses a set of pre-defined signatures based on known malicious network traffic patterns.[5] Einstein 3, the next evolution of the program, will be an intrusion prevention system.[6] Figure 1 illustrates the functionality of Einstein 1 and Einstein 2, the TIC structure, and MOE access points.

[5] Signatures are specific patterns of network traffic that affect the integrity, confidentiality, or availability of computer networks, systems, and information. For example, a specific signature might identify a known computer virus that is designated to delete files from a computer without authorization. Signatures are derived from numerous sources, such as commercial or public computer security information; incidents reported to the US-CERT; information from federal partners; or independent in-depth analyses by US-CERT analysts.

[6] An intrusion prevention system is software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents.

Figure 1: Einstein Data Collection Infrastructure & Process



Within the past year, NCSD has accelerated the deployment of its Einstein technology. As of December 31, 2009, Einstein technology was deployed and operational on networks at 21 agencies. Einstein 1 technology, which will be upgraded to Einstein 2 technology once TIC deployment at those agencies is complete, is deployed at nine federal agencies. Additionally, in the first federal-state partnership of its kind, Einstein 1 was deployed on specified Michigan state government networks in November 2009. Einstein 2 technology is currently deployed and operational at 11 federal agency TIC sites.

Vulnerability information obtained through the Einstein program is shared with stakeholders in the public and private sector through various channels, one of which is the HSIN/US-CERT Portal. The HSIN/US-CERT Portal provides the necessary network and IT infrastructure for US-CERT personnel to share security-related information. The portal is a collaborative system that allows for real-time alerts, notification, and sensitive information sharing. Finally, the NCPS Public Web (www.us-cert.gov) supports US-CERT's mission by serving

as a communications channel to disseminate technical details of internet threats, and guidelines for addressing these threats, to security practitioners.

Results of Audit

System and Physical Security Controls Implemented

The systems utilized by US-CERT are important in helping NCSD meet its mission to protect federal departments and agencies from cyber threats and intrusions. It is imperative that adequate logical security controls be implemented on the department's cybersecurity program systems to ensure that the integrity and reliability of the information processed, stored, and transmitted is not compromised. Physical security controls are needed to protect the systems from unauthorized access, misuse, or destruction. During our audit, we identified the following:

- Adequate system security controls are implemented on three of US-CERT's cybersecurity program systems: NCPS Einstein, HISN/USCERT Portal, and NCPS Public Web. No high-risk or critical security vulnerabilities were identified during our vulnerability scans of these systems.

- Interconnection security agreements (ISA) and comprehensive memorandums of understanding/agreement (MOU/A) that define the roles and responsibilities between DHS and participating agencies for the Einstein program have been established. ISAs are vital in protecting the confidentiality, integrity, and availability of the data processed between interconnected IT systems. An ISA supports a separate MOU/A, which defines the general responsibilities for establishing, operating, and securing a connection. Both ISAs and MOAs must be signed and approved prior to the installation of Einstein sensors on a department/agency network.

- Adequate physical security is implemented at the facilities where the cybersecurity program systems are located. For example, smart cards are required to access facilities that house the MOE and NCPS Einstein. Biometric fingerprint scans are required to access the server room housing HSIN/US-CERT Portal equipment. Warning signs are posted informing personnel that the MOE and NCPS Einstein areas are under 24-hour video surveillance, and the server room is monitored. Figure 2 shows examples of the physical security protective measures observed at the contractor's facility housing the MOE and NCPS Einstein in Florida.

Figure 2: Examples of Physical Security Controls

Server Room Security Camera

Video Surveillance Monitoring Station

Server Room Warning Sign

Server Room Smart Card Reader

The success of NCSD depends in part on its ability to secure the systems used by US-CERT to accomplish its cybersecurity mission. Specifically, the confidentiality, integrity, and availability of the information collected, processed, and disseminated by US-CERT relies on whether adequate security controls have been implemented on DHS' cybersecurity program systems. Although NCSD has implemented adequate physical and logical access controls to secure the systems utilized by US-CERT, security-related issues must be addressed in order to implement a robust program for enhancing the cybersecurity posture of the federal government. For example, NCSD must focus its attention on mitigating vulnerabilities on the MOE and ensuring compliance with Federal Information Security Management Act (FISMA) requirements and DHS IT policies and procedures.

Security Vulnerabilities Need to Be Addressed on the MOE

We identified that the system security controls implemented on NCPS Einstein, HISN/USCERT Portal, and NCPS Public Web adequately protect the data collected, stored, and disseminated. However, adequate security controls have not been implemented on the MOE to protect the

data processed from unauthorized access, use, disclosure, disruption, modification, or destruction.

We conducted technical system security vulnerability scans of the MOE in Florida and Virginia; NCPS Einstein in Florida; HSIN/US-CERT Portal in Virginia; and NCPS Public Web in Pennsylvania. We used Nessus, vulnerability scanning software, to conduct our assessments of the system controls on the cybersecurity program systems at the audit locations we visited.[7] The vulnerabilities identified were classified into high-, medium-, and low-risk categories, based on the severity of the vulnerabilities and damage they could inflict on the systems. Figure 3 shows the number of unique high-, medium-, and low-risk vulnerabilities identified by the system.

Figure 3: Unique Vulnerabilities by System and Severity

	High	Medium	Low	Total
MOE	202	95	243	540
NCPS Einstein	0	8	81	89
HSIN/US-CERT Portal	0	1	10	11
NCPS Public Web	0	2	29	31
Total	202	106	363	671

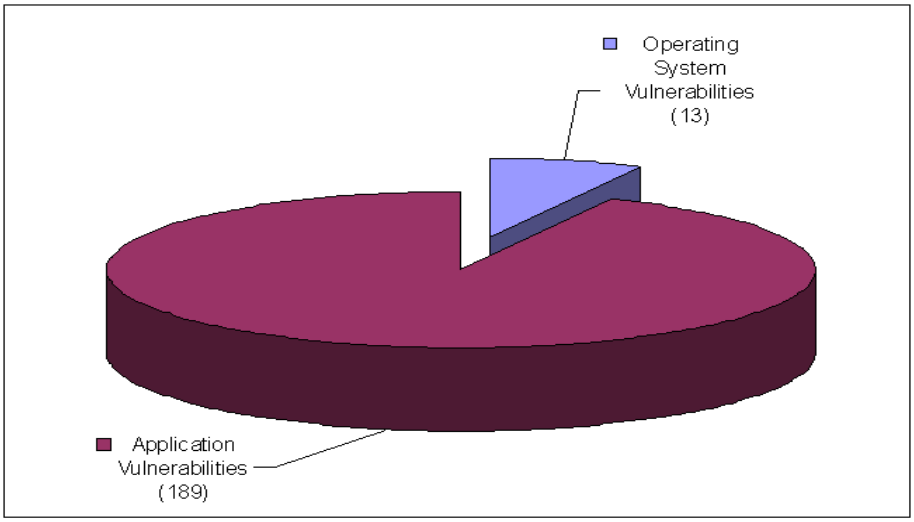
Our scans identified 671 unique vulnerabilities. Existing vulnerabilities can compromise the confidentiality, integrity, and availability of sensitive cybersecurity data. Medium and low-risk vulnerabilities do not pose significant risks; therefore, our analysis of the scan results focused on the 202 unique high risk vulnerabilities identified on the MOE. As previously reported, no significant IT security vulnerabilities were identified from our scans of the NCPS Einstein, HSIN/US-CERT Portal, or NCPS Public Web computers.

Overall, we identified 1,085 instances of high-risk vulnerabilities on the MOE; 202 were unique across 174 MOE computers scanned. The majority of the high-risk vulnerabilities involved application and operating system and security software patches that had not been deployed on MOE computer systems located in Virginia.

[7] Nessus (Professional Feed) is an up-to-date, remote vulnerability scanner for Windows, Linux, Berkeley Software Distribution, Solaris, Apple, and other systems. It is multithreaded, plug-in-based, and currently performs more than a thousand remote security checks.

The application vulnerabilities identified in our scans of the MOE, which NCSD uses for email service and access to NCPS Einstein data, include those involving Microsoft applications, Adobe Acrobat, and Sun Java. Operating system vulnerabilities we identified were related to the Windows and Redhat Linux operating systems. As illustrated in Figure 4, 189 of the 202 unique high-risk vulnerabilities identified were related to applications on the MOE, while the remaining 13 vulnerabilities were identified as operating system vulnerabilities.

Figure 4: Application and Operating System Vulnerabilities



In *The Top Cyber Security Risks*, as reported by the SysAdmin, Audit, Network, Security (SANS) Institute, addressing application vulnerabilities that remain unpatched should be the number one priority for system security personnel, administrators, and owners in 2010.[8] According to SANS data, the number of vulnerabilities being discovered in applications is far greater than the number of vulnerabilities discovered in operating systems.[9] As a result, more exploitation attempts are recorded on application programs, especially email attacks that exploit vulnerabilities in commonly used software and programs such as Adobe and Microsoft Office. Though application attacks are on the rise, operating system attacks are still a security concern; more than 90% of operating system

[8] The SANS Institute is a well-known, cooperative research company that develops and maintains the largest collection of research documents about various aspects of information security and operates the Internet Storm Center, the internet's early warning system.

[9] The SANS Institute's conclusions are based on attack data from TippingPoint intrusion prevention systems protecting 6,000 companies and government agencies, vulnerability data from scans of 9,000,000 systems compiled by Qualys, and additional analysis by key SANS faculty members and the Internet Storm Center.

attacks involve buffer overflow vulnerabilities against Windows operating systems.

The rationale for targeting a particular application or operating system often depends on factors including the prevalence of security vulnerabilities and the inability to effectively patch. Applying patches can reduce the number of vulnerabilities that may affect a system's security posture. In addition, patches are produced and released to add or update features and address security vulnerabilities. The results of our vulnerability assessments revealed that NCSD is not applying timely security and software patches on the MOE. MOE application and operating system vulnerabilities that are not mitigated could compromise the Einstein data accessed through the system.

DHS requires components to reduce vulnerabilities through vulnerability testing and management, the prompt installation of patches, and elimination or disabling of unnecessary services. In addition, according to the National Institute of Standards and Technology (NIST), security and software patches on operating systems and applications should be kept fully up-to-date.

While NCSD performs vulnerability testing and has established a patch management process, the process is ineffective because the vulnerabilities identified are not being properly managed and mitigated in a timely manner on the MOE. According to NCSD, MOE application patches are currently being applied manually. Because of the difficulty in patching a large number of machines manually, patches are often not applied universally, to all computer systems on the network, in a timely fashion. Issues concerning NCSD's MOE patching process, first identified during an April 2009 National Security Agency review, have not yet been addressed.

NCSD's difficulty and inability to timely deploy patches led to our discovery of a high number of application and operating system vulnerabilities that leave the MOE vulnerable to potential attacks. These vulnerabilities, if not addressed, could lead to arbitrary code execution, buffer overflow, escalation of privileges, and denial-of-service attacks. Additionally, since US-CERT analysts gain access to Einstein data via the MOE, the vulnerabilities may put sensitive Einstein data at risk.

We discussed the vulnerabilities identified and provided NCSD system personnel with the technical results from our scans. Using this information, NCSD's system personnel have begun taking actions needed to mitigate the vulnerabilities we identified.

Recommendations

We recommend that the NCSD Director:

Recommendation #1: Mitigate the vulnerabilities identified during the audit to secure the operating systems and applications deployed on the MOE network.

Recommendation #2: Implement a software management solution that will automatically deploy operating system and application security patches and updates on all MOE computer systems to mitigate current and future vulnerabilities.

Management Comments and OIG Analysis

NPPD concurred with recommendation 1. Based on NPPD's response, NCSD has mitigated the identified vulnerabilities. NCSD performed a subsequent scan of the MOE network demonstrating this mitigation and will provide the OIG with a copy of the results.

OIG Analysis

We agree that the steps NCSD has taken satisfy this recommendation. This recommendation will remain open until NCSD provides documentation to support that all planned corrective actions are completed.

NPPD concurred with recommendation 2. Prior to the OIG engagement, NCSD began the acquisition process for a software management solution. Following the acquisition process, NCSD began testing the system, which was deployed on June 30, 2010. NCSD will be demonstrating this system for the OIG for confirmation that responsive action has been taken.

OIG Analysis

We agree that the steps NCSD has taken satisfy the intent of this recommendation. This recommendation will remain open until NCSD provides documentation to support that all planned corrective actions are completed.

FISMA Requirements Are Not Being Met

NCSD is not adhering to FISMA requirements in a number of areas. Specifically, the division has not properly developed or periodically updated the status of known security weaknesses for its cybersecurity program systems in its Plans of Action and Milestones (POA&M). In addition, NCSD has not established an information security training program to ensure that systems personnel and contractors receive adequate security awareness and specialized role-based training commensurate with their specific responsibilities.

FISMA requires each agency to develop, document, and implement an agency-wide information security program to provide a high level of security for the information and information systems that support agency operations and assets. FISMA provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. The act also provides for the development and maintenance of minimum controls required to protect federal information systems and serves as a mechanism for improved oversight of federal agency information security programs. Specifically, FISMA requires agencies to:

- Periodically test and evaluate the effectiveness of information security policies, procedures, and practices.
- Develop and implement a corrective action plan for information system vulnerabilities. This plan, known as a POA&M, is intended to serve as an authoritative management tool to address any security-related weaknesses and deficiencies.
- Provide security awareness training to inform personnel, including contractors and other users of information systems, about the information security risks associated with their activities and their responsibilities in complying with agency policies and procedures designed to reduce these risks.

According to DHS policy, all components must comply with FISMA requirements in establishing their information security programs, and managing and protecting sensitive systems.

NCSD Has Not Developed POA&Ms for Known Vulnerabilities

NCSD is not developing, updating, and tracking the remediation status of its vulnerabilities in POA&Ms for all known IT security weaknesses for the systems included in our audit. For example:

- Although NCSD identified system and security weaknesses in the risk assessment conducted for NCPS Einstein, the POA&M was

not updated to include the vulnerabilities and weaknesses identified. Therefore, NCSD management has no way of knowing whether these weaknesses have been mitigated. Specifically, the risk assessment identified 12 vulnerabilities for Einstein, of which 6 were not accepted risks. In compliance with FISMA and DHS requirements, the six known system security weaknesses should be documented and tracked in a POA&M.

- We compared the results of our system vulnerability scans conducted on January 12, 2010, with the results of system scans NCSD conducted on July 1, 2009, for the MOE in Florida. In comparing the scanning results, we discovered several high risk vulnerabilities that were present on both scans, which indicated that known high risk vulnerabilities had been identified by NCSD and were present on the system for a 6-month period. NCSD should have captured these high risk vulnerabilities in a POA&M when they were identified. However, these vulnerabilities were not documented or tracked in a system POA&M, and therefore, had not yet been mitigated.

POA&Ms provide a means to identify and resolve information security weaknesses and are used to capture and track security weaknesses in information systems. NCSD management may not be aware that system vulnerabilities and security weaknesses exist if they are not properly documented and captured in POA&Ms. Additionally, without this documentation, sufficient resources cannot be dedicated to address weaknesses within a reasonable timeframe. The proper documentation for tracking system vulnerabilities in the POA&Ms would help NCSD management ensure that known system and security vulnerabilities are mitigated.

According to an NCSD management official, the POA&Ms for the MOE and NCPS Einstein were not updated to include system vulnerabilities and weaknesses identified due to poor communication between the technical individuals responsible for conducting vulnerability analyses and personnel responsible for creating POA&Ms. Without proper communication, a plan cannot be created and implemented to mitigate identified vulnerabilities, potentially putting the security of the systems and sensitive cybersecurity data at risk.

NCSD Has Not Established a Formal Information Security Training Program

NCSD has not established a process to ensure that systems personnel and contractors receive required security awareness training or adequate specialized role-based training commensurate with their specific

responsibilities. Specifically, NCSD has not identified the required security courses or areas of focus for its system administrators and contractors. Furthermore, NCSD has not designated a coordinator to monitor personnel training and maintain records to ensure that its administrators, employees, and contractors receive security awareness training and specialized training that meets the specific needs for their roles and the division.

NCSD management maintains that employees are responsible for determining their own training needs and maintaining training records. Though NCSD personnel have taken specialized training, a listing of specific required or recommended specialized training courses for systems personnel or contractors has not been developed.

FISMA requires agencies to provide employees, contractors, and other users of information systems with security awareness training. This training should inform them about the risks associated with their activities when accessing government information systems and their responsibilities in complying with agency policies and procedures designed to reduce these risks. DHS requires components to establish an information security training program for its users of DHS information systems. Components are required to establish an overall policy for information security awareness, training, and education, which includes providing guidance on preparing and attending security awareness and training sessions. Component Chief Information Security Officers and Information Systems Security Managers are to ensure training and oversight for personnel with significant responsibilities for information security and maintain training records for system personnel and contractors. Furthermore, NIST recommends that management determine staff training needs, prioritize the use of training resources, and evaluate training effectiveness.

Without a formal training process and management oversight, NCSD's system administrators and contractors may not possess the professional qualifications required to administer the division's systems. In addition, system personnel and contractors may not develop the skills/knowledge needed to maintain and improve system operations. Training will assist NCSD personnel in obtaining knowledge about current security threats, risks, trends, and mitigation techniques. NCSD cannot effectively execute its mission while protecting the integrity, confidentiality, and availability of information in today's highly networked system environment without ensuring that each person involved understands their roles and responsibilities and is adequately trained to perform them.

Recommendations

We recommend that the NCSD Director:

Recommendation #3: Create POA&Ms for known security vulnerabilities, assign appropriate resources, and monitor the progress of corrective actions until risks are mitigated.

Recommendation #4: Establish an information security training process that includes developing a list of required and recommended courses for NCSD systems personnel and contractors, monitoring training taken, and maintaining course records. This should help to ensure that systems personnel and contractors receive security awareness training and specialized training commensurate with their roles and responsibilities.

Management Comments and OIG Analysis

NPPD concurred with recommendation 3. Although NCSD undertakes these activities, it will improve risk mitigation processes. The NCSD-Information Assurance (IA) team regularly initiates and tracks POA&Ms for each NCSD IT system. Findings that can be mitigated within a short amount of time (one week) are not uploaded onto Trusted Agent FISMA (TAF). However, where POA&M items cannot be mitigated within a short period, a waiver or exception is requested from NPPD's Office of the Chief Information Officer and the action is included in the overall system POA&M. NCSD is improving its internal processes to ensure that POA&Ms are created after each scan, or when otherwise appropriate.

OIG Analysis

We agree that the steps NCSD plans to take satisfy the intent of this recommendation. This recommendation will remain open until NCSD provides documentation to support that all planned corrective actions are completed.

NPPD concurred with recommendation 4. NCSD recognizes the value in identifying role-based training requirements for all employees and is developing a process to identify information security training requirements for NCSD employees.

The types of training and certifications for which a process will be developed include training and requirements currently being met by NCSD personnel, such as the DHS-wide annual Security

Education Awareness and Training requirement, which is already tracked and monitored by NPPD; the DHS-sponsored Critical Control Review and Document Review training; the CISSP Boot Camp; and Security Plus training, along with other role-based training.

OIG Analysis

We agree that the steps NCSD has taken, and plans to take, satisfy the intent of this recommendation. This recommendation will remain open until NCSD provides documentation to support that all planned corrective actions are completed.

System and Program Documentation Has Not Been Reviewed or Approved

NCSD's information systems security management staff has not reviewed and approved required system certification and accreditation documentation, or the division's policies and standard operating procedures (SOP) for its cybersecurity program. In addition, the Fiscal Year (FY) 2010 annual system self-assessments conducted for the division's cybersecurity systems are incomplete.

NCSD's Information Systems Security Manager is to review and approve system documentation prior to certifying it for accreditation by the Designated Approving Authority. Division and program system security policies and procedures should not be implemented until they have been approved by the appropriate management officials. Appropriate policies, procedures, and system certification and accreditation security documentation should be completed and approved to efficiently execute the NCPS Einstein program and secure the cybersecurity program systems.

NCSD has drafted all documentation required for the certification and accreditation of its cybersecurity program systems. However, a significant amount of this documentation has not been reviewed or approved by management. Documents in draft form include the system security plans (SSP) and security test and evaluations (ST&E) for all four of the cybersecurity program systems included in our audit; the HSIN/US-CERT Portal Contingency Plan; and the NCPS Public Web Security Assessment Report and Contingency and Disaster Recovery Plan. In addition, division and program procedures and policies for discretionary access control, incident handling and reporting, and data management have not been reviewed or approved by management.

Furthermore, though NCSD has drafted its FY 2010 annual self-assessments for the cybersecurity program systems, the supporting documentation for these assessments is incomplete. For example, the assessments do not contain information regarding the system environment or stipulate the regulations, laws, and policies related to the systems. Required appendices for system acronyms, definitions, and references have not been completed. In addition, the list of interconnected systems in the NCPS Einstein annual self-assessment is outdated.

DHS requires that risk assessments, SSPs, and ST&Es for the certification and accreditation package be approved by the system owner and agreed to by the certifying official before a system is certified and accredited. Components are to periodically test the security of implemented systems, and Information Systems Security Managers are required to validate all component information system security reporting. Component personnel must review ISAs as part of their annual self-assessment.

According to an NCSD official, management turnover has caused a delay in getting program and system documentation reviewed and approved. As a result, system certification and accreditation documentation, as well as NCSD's policies and SOPs, have not been reviewed to determine whether they are adequate and in compliance with DHS requirements. As a result, management cannot ensure that policies/procedures and security controls, when implemented, will allow for the efficient execution of NCSD operations and the NCPS Einstein program, or that its cybersecurity program data and systems are adequately secured.

Recommendations

We recommend that the NCSD Director:

Recommendation #5: Review and approve program and system documentation for its cybersecurity program.

Recommendation #6: Update the annual system self-assessments for the division's cybersecurity systems to include all system information and complete the appendices according to DHS requirements.

Management Comments and OIG Analysis

NPPD concurred with recommendation 5. SOP and Certification and Accreditation (C&A) documents for NCSD IT systems undergo several reviews before uploaded into TAF. C&A documentation is reviewed and approved at various levels beginning with the network manager, system owner, and the

NCSD Information System Security Officer. Once C&A documents are uploaded into TAF, the NPPD Information System Security Manager, NPPD Designated Accrediting Authority, and DHS Headquarters provide validation, which signifies approval. SOPs are developed either by the operations or IA team, and are coordinated with both teams prior to being sent to the Logistics Lead for senior leadership coordination, approval, implementation, and maintenance. Going forward, SOPs will clearly indicate date of approval and will include the signature of the appropriate team lead (either operations or IA, as appropriate). NPPD and NCSD will improve the documentation of these reviews, approvals and validations.

OIG Analysis

We agree that the steps NCSD is taking, and plans to take, satisfy the intent of this recommendation. This recommendation will remain open until NCSD provides documentation to support that all planned corrective actions are completed.

NPPD concurred with recommendation 6. In accordance with DHS Sensitive System Handbook 4300A Section 3.9.12, requiring completion of annual assessments, and further described in the DHS Fiscal Year 2010 DHS Information Security Performance Plan (October 1, 2009), NCSD completes annual assessments in accordance with DHS requirements, which are established by the DHS Chief Information Security Officer. As required, NCSD's annual assessments for all NCPS systems, which include the MOE, EINSTEIN, the US-CERT, and HSIN portals, and US-CERT's public website, were approved and validated by the end of February 2010. NCSD however will update its system self-assessments to include missing system information and completed appendices.

OIG Analysis

We agree that the steps NCSD plans to take satisfy the intent of this recommendation. This recommendation will remain open until NCSD provides documentation to support that all planned corrective actions are completed.

NCSD Is Not Fully Complying with DHS Policies

NCSD is not fully complying with DHS policies governing sensitive systems. Specifically, the division is not complying with DHS Sensitive Systems Policy Directive 4300A criteria for firewall testing, Secure Baseline Configuration Guides (SBCG), and physical security of server rooms. DHS Sensitive Systems Policy Directive 4300A provides baseline policies, standards, and guidelines for DHS components. It provides direction to managers and senior executives for managing and protecting sensitive systems. The policies and direction contained in the directive apply to all DHS components.

Firewall Testing

NCSD is not adhering to DHS Directive 4300A requirements for firewall testing. DHS 4300A requires that all components conduct quarterly firewall tests to ensure that firewall configurations are properly applied to all systems. According to NCSD systems personnel, firewall tests were conducted on the cybersecurity program systems included in our audit. However, NCSD was unable to provide us with the dates that the firewalls were last tested or documentation to support that firewall tests were conducted. NCSD cannot ensure that firewalls are operating properly to protect systems from unauthorized access attempts if it does not adequately test firewall configurations.

SBCG Criteria

NCSD is not following the DHS SBCGs. Instead, the division uses the Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGS) to configure its systems' hardware and software components.[10] NCSD has hardened its routers, servers, and workstations for its cybersecurity program systems based on the STIGs. However, we identified a few instances of noncompliance in areas related to password management, logon settings, event logging, port management, service management, and shutdown procedures. It is important for components to follow the proper hardening guides to ensure that systems and devices are securely configured throughout the department, and data is protected according to department policies.

We discussed areas of noncompliance with NCSD's system personnel. Since conducting our evaluation of NCSD's compliance with the SBCGs, management has taken actions to ensure that system configuration settings are aligned with DHS requirements.

[10] DHS' SBCGs are constructed from configuration management policies in the STIGS, along with standards from NIST and Microsoft.

Server Room Security

Generally, the facilities housing cybersecurity program systems equipment are secure. Still, system personnel responsible for the HSIN/US-CERT Portal can improve security by conducting formal inspections of offices and areas housing system equipment as required by DHS. These inspections can ensure that physical security safeguards are working properly and policies are being followed to protect systems from threats associated with the physical environment and prevent unauthorized access, disclosure, destruction, or modification.

Further, to avoid potential damage to equipment that is critical in carrying out DHS' cybersecurity program, NCSD needs to establish a policy and procedures that can be taken when the temperature and humidity inside its server rooms, which are operational 24 hours a day/7 days a week, fall outside of the department's acceptable range. DHS requires the temperature in server rooms to be between 60 and 70 degrees, while the humidity should be between 35% and 65%. When we conducted a physical security evaluation of the NCPS Einstein system in Florida, on February 23, 2010, the four computer consoles in the server room recorded temperatures of 40 degrees, 75 degrees, 77 degrees, and 82 degrees. The humidity in the server room was 78%.

According to NCSD system personnel, the temperature was high because the "chiller" was not operational. According to management, the "chiller" was repaired February 24, 2010. During this time, the climate changes in NCSD's server room in Florida could have potentially put NCPS Einstein data at risk.

When the temperature and humidity readings of equipment in the server room rise above the normal range required by DHS, industry best practices recommend that the equipment be shut down until climate issues are resolved. Shutting down the equipment would prevent the danger of the equipment overheating or malfunctioning.

Recommendations

We recommend that the NCSD Director:

Recommendation #7: Conduct and document quarterly firewall testing to ensure that cybersecurity program systems are protected from possible unauthorized access attempts.

Recommendation #8: Implement DHS baseline configuration settings on its routers, servers, and workstations for its cybersecurity program.

Recommendation #9: Conduct and document physical security inspections of offices and areas housing system equipment according to DHS policy. This will help to ensure that physical security safeguards are working properly and policies are being followed.

Recommendation #10: Establish a policy and institute procedures that can be taken to prevent potential damage to DHS equipment when the temperature or humidity inside server rooms fall outside of the department's acceptable range.

Management Comments and OIG Analysis

NPPD concurred with recommendation 7. NCSD tests firewalls at least quarterly, but agrees that a documentation process will allow better management oversight of such testing. An SOP for firewall testing has been developed and a copy was provided to the OIG.

OIG Analysis

NCSD provided a copy of the signed SOP on July 9, 2010. The documentation provided satisfies the intent of this recommendation. We consider this recommendation resolved and closed.

NPPD concurred with recommendation 8. DHS baseline configuration settings are now implemented across NCSD's systems. Consistent with DHS Sensitive System Handbook 4300A, Section 4.8.4, DHS SBCGs provide a minimum baseline of security. That is the basis upon which NCSD's equipment is prepared for deployment. Section 4.8.4 allows DHS Components to "implement more onerous configuration guides" and, to that end, NCSD relies upon the DISA STIGs to supplement configuration settings. The STIGs are used as an automated tool for configuration management.

OIG Analysis

We agree that the steps NCSD has taken satisfy the intent of this recommendation. This recommendation will remain open until NCSD provides documentation to support that all planned corrective actions are completed.

NPPD concurred with recommendation 9. Such inspections generally are already conducted and documented, and NCSD will

work with its partners to ensure that this practice is followed and documented at each office and for area housing system equipment.

OIG Analysis

We agree that the steps NCSD plans to take satisfy the intent of this recommendation. This recommendation will remain open until NCSD provides documentation to support that all planned corrective actions are completed.

NPPD concurred with recommendation 10. DHS Sensitive System Handbook 4300A, Section 4.2.1.8, directs DHS components to consider maintaining a temperature range between 60 and 70 degrees and humidity levels between 35% and 65% when developing a strategy for temperature and humidity control. The handbook further recommends checking individual system documentation for the proper temperature and humidity levels. NCSD will establish a temperature and humidity policy, which incorporates DHS and equipment manufacturer guidance, and the division will institute procedures to take when temperature or humidity is out of tolerance.

OIG Analysis

We agree that the steps NCSD plans to take satisfy the intent of this recommendation. NCSD's policy should be updated once a backup site for operations has been established. This recommendation will remain open until NCSD provides documentation to support that all planned corrective actions are completed.

The objective of our audit was to determine whether adequate physical and logical access controls are in place to secure the cybersecurity program systems utilized by US-CERT and safeguard the data collected and disseminated by US-CERT. Specifically, we:

- Determined what and how cybersecurity data is collected and maintained by US-CERT.
- Evaluated the adequacy of physical security controls implemented to protect NCSD's cybersecurity program systems.
- Determined whether US-CERT has implemented effective system security controls to safeguard the confidentiality, integrity, and availability of cybersecurity data.
- Determined whether the system documentation for DHS' cybersecurity program systems has been completed in compliance with DHS and FISMA requirements.

Our audit focused on the requirements outlined in Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*; OMB M-08-05, *Implementation of Trusted Internet Connections (TIC)*; NIST Special Publication (SP) 800-16, *Information Technology Security Training Requirements: A Role and Performance-Based Model*; NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*; NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems*; NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment;* FISMA; Government Performance Results Act of 1993; DHS Sensitive Systems Policy Directive 4300A; DHS 4300A Sensitive Systems Handbook; DHS Windows Server 2003 SBCG; DHS Linux SBCG; DHS Windows XP SBCG; and DHS CISCO Router SBCG.

We reviewed and evaluated NCSD's SOPs, policies, and guidelines, including NCSD's discretionary access control policy, interconnection security agreements, and memorandums of agreement. We also reviewed system certification and accreditation documentation, including POA&Ms for the MOE, NCPS Einstein, HSIN/US-CERT Portal, and NCPS Public Web, for compliance with applicable OMB, NIST, and DHS guidance.

We interviewed selected personnel from NCSD and US-CERT, including NCSD program management officials; Information System Security Officers; Physical Facility Security Managers; system administrators; and contractor personnel. We conducted physical security evaluations at contractor facilities in Florida and Virginia, and at NCSD headquarters. Furthermore, we performed detailed vulnerability assessments to evaluate the effectiveness of the system security controls implemented, reviewed system configuration requirements, and verified account management and

access control procedures for NCSD's cybersecurity program systems (MOE, NCPS Einstein, HSIN/US-CERT Portal, and NCPS Public Web). We reviewed NCSD's vulnerability assessments and compared them with our own assessments to determine whether known systems and security vulnerabilities had been mitigated.

We conducted this performance audit at NCSD headquarters and contractor facilities in Florida, Pennsylvania, and Virginia between January 2010 and May 2010 pursuant to the *Inspector General Act of 1978*, as amended, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives. Major OIG contributors to the audit are identified in Appendix C.

The principal OIG points of contact for the audit are Frank Deffer, Assistant Inspector General, IT Audits, at (202) 254-4100, and Chiu-Tong Tsang, Director, Information Security Audit Division, at (202) 254-5472.

Appendix B
Management Comments to the Draft Report

Office of the Under Secretary
National Protection and Programs Directorate
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

JUL 30 2010

MEMORANDUM TO: Frank Deffer
Assistant Inspector General

FROM: Rand Beers
Under Secretary

SUBJECT: Response to Office of Inspector General Draft Report "*DHS Needs to Improve the Security Posture of its Cybersecurity Program Systems*"

This correspondence responds to your June 11, 2010 memorandum requesting that the National Protection and Programs Directorate (NPPD) provide comments on the Office of Inspector General (OIG) draft report titled *DHS Needs to Improve the Security Posture of its Cybersecurity Program Systems.*

Responses to the ten recommendations directed to NPPD are set forth below. Technical comments are being provided under separate cover. Questions concerning specific comments should be addressed to Michael McPoland, Director, NPPD GAO-OIG Audit Liaison Office at (703) 235-2175.

Recommendation 1: *Ensure that the vulnerabilities identified during the audit are mitigated to secure the operating systems and applications deployed on the MOE network.*

Response: NPPD concurs with this recommendation and the National Cyber Security Division (NCSD) has mitigated the identified vulnerabilities. NPPD believes this recommendation should be closed. A subsequent scan of the Mission Operating Environment (MOE) network demonstrating this mitigation is being delivered to OIG.

Recommendation 2: *Implement a software management solution that will automatically deploy operating system and application security patches and updates on all MOE computer systems to mitigate current and future vulnerabilities.*

Response: NPPD concurs with this recommendation. Prior to this OIG engagement, NCSD began the acquisition process for such a software management solution. Following the acquisition process, NCSD began testing the system, which was deployed on June 30, 2010. NCSD is demonstrating this system to OIG for confirmation that responsive action has been taken.

Recommendation 3: *Create POA&Ms for known security vulnerabilities, assign appropriate resources, and monitor the progress of corrective actions until risks are mitigated.*

Response: NPPD concurs with this recommendation. Although NCSD undertakes these activities, it will improve risk mitigation processes. The NCSD-Information Assurance (IA) team regularly initiates and tracks Plan of Action and Milestones (POA&Ms) for each NCSD information technology system. Findings that can be mitigated within a short amount of time (one week) are not uploaded onto Trusted Agent FISMA (TAF). However, where POA&M items cannot be mitigated within a short period, a waiver or exception is requested from the NPPD's Office of the Chief Information Officer and the action is included in the overall system POA&M. NCSD is improving its internal processes to ensure that POA&Ms are created after each scan, or when otherwise appropriate.

Recommendation 4: *Establish an information security training process that includes developing a list of required and recommended courses for NCSD systems personnel and contractors, monitoring training taken, and maintaining course records to ensure that systems personnel and contractors receive security awareness training and specialized training commensurate with their roles and responsibilities.*

Response: NPPD concurs with this recommendation. NCSD recognizes the value in identifying role-based training requirements for all employees and is developing a process to identify information security training requirements for NCSD employees.

The types of training and certifications for which a process will be developed include training and requirements currently being met by NCSD personnel, such as the Department of Homeland Security (DHS)-wide annual Security Education Awareness and Training (SEAT) requirement, which is already tracked and monitored by NPPD; the DHS-sponsored Critical Control Review and Document Review training; the CISSP Boot Camp; and Security Plus training, along with other role-based training.

Recommendation 5: *Ensure that program and system documentation for its cybersecurity program systems is reviewed and approved.*

Response: NPPD concurs with this recommendation. Standard operating procedures and Certification and Accreditation (C&A) documents for NCSD IT Systems undergo several reviews before being uploaded into TAF. C&A documentation is reviewed and approved at various levels beginning with the network manager, system owner, and the NCSD Information Systems Security Officer. Once C&A documents are uploaded into TAF, the NPPD Information System Security Manager (ISSM), NPPD Designated Accrediting Authority and DHS Headquarters provide validation, which signifies approval. Standard Operating Procedures (SOPs) are developed either by the operations or IA team, and are coordinated with both teams prior to being sent to the Logistics Lead for senior leadership coordination, approval, implementation and maintenance. Going forward, SOPs will clearly indicate date of approval and will include the signature of the appropriate team lead (either operations or IA, as appropriate). NPPD and NCSD will improve the documentation of these reviews, approvals and validations.

Recommendation 6: *Ensure the annual system self-assessments for the division's cybersecurity systems are updated to include all system information and that appendices are completed according to DHS requirements.*

Response: NPPD concurs with this recommendation. In accordance with DHS Sensitive System Handbook 4300A Section 3.9.12, requiring completion of annual assessments, and further described in the DHS Fiscal Year 2010 DHS Information Security Performance Plan (October 1, 2009), NCSD completes annual assessments in accordance with DHS requirements, which are established by the DHS Chief Information Security Officer. As required, NCSD's annual assessments for all National Cybersecurity Protection System (NCPS) systems, which include the MOE, EINSTEIN, the US-CERT and Homeland Security Information Network portals, and US-CERT's public website, were approved and validated by the end of February 2010. NCSD however will update its system self-assessments to include missing system information and completed appendices.

Recommendation 7: *Ensure quarterly firewall testing is conducted and documented to ensure that cybersecurity program systems are protected from possible unauthorized access attempts.*

Response: NPPD concurs with this recommendation. NCSD tests firewalls at least quarterly, but agrees that a documentation process will allow better management oversight of such testing. A standard operating procedure for firewall testing has been developed and a copy was provided to the OIG.

Recommendation 8: *Ensure that DHS baseline configuration settings are fully implemented on its routers, servers, and workstations for its cybersecurity program.*

Response: NPPD concurs with this recommendation. DHS baseline configuration settings are now implemented across NCSD's systems. Consistent with DHS Sensitive System Handbook 4300A, Section 4.8.4, DHS Secure Baseline Configuration Guides provide a minimum baseline of security. That is the basis upon which NCSD's equipment is prepared for deployment. Section 4.8.4 allows DHS Components to "implement more onerous configuration guides" and, to that end, NCSD relies upon the Defense Information Systems Agency's Security Technical Implementation Guides (DISA STIGs) to supplement configuration settings. The STIGs are used as an automated tool for configuration management. In fact, since automated tools are required for use by DHS, based on NIST 800-53, Rev 3, Control CM-2 and Control Enhancement (2), and the DHS baseline guides provide only a manual checklist, use of the DISA STIGs is preferred.

To ensure that this practice is more clearly articulated, NCSD will reflect it in its configuration SOP.

Recommendation 9: *Conduct and document physical security inspections of offices and areas housing system equipment according to DHS policy, at all locations, to ensure that physical security safeguards are working properly and policies are being followed.*

Response: NPPD concurs with this recommendation. Such inspections generally are already conducted and documented, and NCSD will work with its partners to ensure that this practice is followed and documented at each office and for area housing system equipment.

Recommendation 10: *Establish a policy and institute procedures than can be taken to prevent potential damage to DHS equipment if the temperature and/or humidity inside server rooms fall outside of the department's acceptable range.*

Response: NPPD concurs with this recommendation. DHS Sensitive System Handbook 4300A, Section 4.2.1.8, directs DHS components to consider maintaining a temperature range between 60 and 70 degrees and humidity levels between 35% and 65% when developing a strategy for temperature and humidity control. The handbook further recommends checking individual system documentation for the proper temperature and humidity levels. NCSD will establish a temperature and humidity policy, which incorporates DHS and equipment manufacturer guidance, and the division will institute procedures to take when temperature or humidity is out of tolerance.

Thank you for the opportunity to review and comment on this draft report. We look forward to continuing this partnership in the future.

Information Security Audit Division

Chiu-Tong Tsang, Director
Barbara Bartuska, IT Audit Manager
Charles Twitty, Senior Auditor/Team Lead
Bridget Glazier, IT Auditor
Thomas Rohrback, IT Specialist
David Bunning, IT Specialist

Erin Dunham, Referencer

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretariat
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Deputy Under Secretary, NPPD
Assistant Secretary, Cyber Security and Communications
Chief Information Officer
Chief Security Officer
Chief Information Security Officer
Director, NCSD
Deputy Director, NCSD
Director, Network Security Development, NCSD
Deputy Director, US-CERT
Chief Information Officer, NPPD
Director, IT Security, NPPD
Director, Departmental GAO/OIG Liaison Office
Director, Compliance and Oversight Program
Deputy Director, Compliance and Oversight
Audit Liaison, NPPD
Audit Liaison, NCSD
Audit Liaison, Chief Information Officer
Audit Liaison, Chief Information Security Officer
Director, Information Security Audit Division
IT Audit Manager, Information Security Audit Division

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4305, or visit the OIG web site at www.dhs.gov/oig.

OIG HOTLINE

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations:

- Call our Hotline at 1-800-323-8603;
- Fax the complaint directly to us at (202) 254-4292;
- Email us at DHSOIGHOTLINE@dhs.gov; or
- Write to us at:
  DHS Office of Inspector General/MAIL STOP 2600,
  Attention: Office of Investigations - Hotline,
  245 Murray Drive, SW, Building 410,
  Washington, DC 20528.

The OIG seeks to protect the identity of each writer and caller.