DEPARTMENT OF JUSTICE EFFORTS IN MANAGING INFORMATION TECHNOLOGY SECURITY VULNERABILITIES

U.S. DEPARTMENT OF JUSTICE

OFFICE OF THE INSPECTOR GENERAL
AUDIT DIVISION

AUDIT REPORT 09-04

DECEMBER 2008

REDACTED – FOR PUBLIC RELEASE

DEPARTMENT OF JUSTICE EFFORTS IN MANAGING INFORMATION TECHNOLOGY SECURITY VULNERABILITIES*

EXECUTIVE SUMMARY

The Department of Justice (Department), like the rest of the federal government has become increasingly dependent on information technology (IT) systems to accomplish its mission. These systems contain a wide range of data regarding individuals, organizations, and other sensitive information. Any IT system inherently contains vulnerabilities that, if exploited, can expose sensitive information to unauthorized individuals, and in some cases compromise national security. To reduce the risk of compromise of its IT systems and the data they contain, it is essential that the Department minimize the vulnerabilities in its IT systems. Enhancing the security of the information contained within its IT systems is a top priority of the federal government and the Department.

To assist federal agencies in securing IT systems and to help provide a framework to protect federal information resources that support federal operations, Congress passed the *Federal Information Security Management Act of 2002* (FISMA).[1] FISMA established federal information security program evaluation and reporting requirements that are primarily aimed at ensuring that government agencies have established policies and procedures to enhance the security of the information contained in their IT systems. FISMA also resulted in criteria against which federal agencies are evaluated and graded regarding the development of policies and procedures to secure IT systems.

In May 2008, the Department received an A^+ on the FISMA report card prepared by the House Committee on Oversight and Government Reform.[2] This grade was an improvement over the A^- received for FY 2006 and the D received for FY 2005. The report card grade was based on two annual reports submitted to the Office of Management and Budget (OMB) to measure the Department's compliance with FISMA, one by the Department

---

* The full version of this report includes information that the Department considered sensitive and therefore could not be publicly released. To create this public version of the report the Office of the Inspector General redacted the portions of the full report that the Department considered sensitive and indicated where those redactions were made.

[1] 44 U.S.C. § 3541, *et seq.* (2002).

[2] Federal agencies overall averaged a C for FY 2007.

of Justice Office of the Inspector General (OIG) and one by the Department. The A^+ grade signified the Department had complied with FISMA requirements and developed policies, procedures, and processes that establish information system security requirements for its system inventory; assessed risk; and evaluated security controls in its information systems.

However, neither FISMA nor the A^+ grade measured the effect FISMA compliance had on the actual security of the Department's IT systems. It is important to note that FISMA does not provide a comprehensive view of an agency's information security practices. The Department's A^+ FISMA score demonstrated progress in that the Department has successfully documented the FISMA-required processes, but it is not an assurance that the Department has implemented those processes or adequately secured its IT systems.

Unlike a FISMA review, this audit sought to assess the implementation of the Department's vulnerability management policies and procedures and their effect on the Department's IT security.

OIG Audit Approach

The objectives of this audit were to identify the Department's major systemic IT security vulnerabilities and assess the Department's progress in mitigating the identified vulnerabilities, in monitoring and overseeing the implementation of the IT security program, and in improving the overall security of its IT systems. The scope of our audit was limited to a review of the vulnerability management part of the Department's IT security program, which focuses on addressing the greatest threats to IT systems. We did not review and evaluate the adequacy of other elements of the Department's overall IT security efforts, such as training or contingency planning.

To accomplish the objectives of our review, we interviewed the Department's Chief Information Officer (CIO) and Deputy CIO, as well as CIOs and Information System Security Officers (ISSO) from 10 components within the Department.[3] In addition, we reviewed and evaluated the Department's IT security vulnerability and incident reports from January 1,

[3] We interviewed officials from the Bureau of Alcohol, Tobacco, Firearms and Explosives; Federal Bureau of Prisons; Criminal Division; Drug Enforcement Administration; Executive Office for Immigration Review; Executive Office for United States Attorneys; Executive Office for United States Trustees; Federal Bureau of Investigation; Office of Justice Programs; and United States Marshals Service.

2007, through September 30, 2007.[4] To find obstacles that may impede identification and remediation of vulnerabilities, we also evaluated the procedures used to identify systemic IT security vulnerabilities. Appendix I contains a further description of our audit objectives, scope, and methodology.

Results in Brief

As signified by the A+ FISMA score, the Department has well-documented processes and procedures for its IT vulnerability management program. In addition, the Department has implemented sound processes and procedures for identifying vulnerabilities. However, we found that the Department has not fully implemented the policies and procedures intended to remediate identified vulnerabilities to enhance the security of the Department's IT systems.

Also, our review identified major systemic IT security vulnerabilities such as inadequate access controls, [redacted], and outdated security patches that require immediate attention. Specifically, we determined that the Department lacks effective methodologies for tracking the remediation of IT vulnerabilities identified in the monthly system configuration scans, for applying Department-wide remedies for known vulnerabilities, and for maintaining an inventory of devices connected to the Department's various IT networks.[5]

We also found that the Department's focus on meeting FISMA requirements may have affected its ability to effectively secure its IT security environment. For example, the Department eliminated a requirement for its components to develop mitigation plans for all vulnerabilities identified during the monthly system scans because it was not necessary to meet FISMA requirements. Although removing this requirement did not violate FISMA, it limited the Department's ability to monitor the components' progress in resolving those vulnerabilities and ultimately improve the security of its IT systems.

In this report, we make four recommendations to assist the Department in its efforts to remediate known IT vulnerabilities. These recommendations include establishing a process to monitor the remediation

[4] The IT system vulnerability report contains the results of the monthly system scans of the Department's IT systems and the incident report contains a listing of all reported security incidents – losses of laptops, BlackBerry devices, and system intrusions.

[5] Monthly system configuration scans are periodic checks of a system's security configuration to determine compliance with established requirements.

of IT security vulnerabilities identified during the monthly system scanning process, ensuring remediation efforts are conducted throughout the Department, and performing an inventory of all IT devices on the Department's networks to ensure that the monthly system scans represent the Department's entire IT environment.

Our report contains detailed information on the full results of our review of the Department's efforts to manage its IT security vulnerabilities. The remaining sections of this Executive Summary describe in more detail our audit findings.

Status of the Department's IT Vulnerability Management

The core of an agency's information security program is vulnerability management, which is the process used to determine whether to eliminate, mitigate, or accept vulnerabilities based on risk and cost. This process is intended to make IT environments more secure and to improve an agency's regulatory compliance.

To govern its vulnerability management program, the Department has documented its vulnerability management policies and procedures in a Vulnerability Management Plan (VM Plan).[6] As a result of the quality and completeness of this document, the Department received an A^+ on its FISMA report card. The VM Plan consolidates the Department's requirements for vulnerability scanning, reporting, and compliance validation and is used by security and operations personnel throughout the Department.

The Department also implemented the Cyber Security Assessment and Management (CSAM) automated tool kit to manage the implementation of the VM Plan requirements and to meet the FISMA reporting requirements.[7] The Department uses the information in CSAM to assess a system's security as corrective actions are completed.

We found that the Department successfully implemented the requirements for vulnerability identification, but has struggled with

---

[6] The document is entitled Foundstone Vulnerability Management Compliance and Validation, Version 2, March 9, 2007. The Department uses the Foundstone Enterprise (Foundstone) software package to administer the vulnerability management plan. Foundstone, which is distributed by McAfee Security Services, identifies vulnerabilities and assigns risk factors based on the extent of possible harm that could be caused if the vulnerabilities were exploited.

[7] CSAM is the Department's FISMA compliance, management, and automated reporting tool that is used to monitor FISMA compliance and vulnerability remediation.

implementing the requirements for mitigating those vulnerabilities after they are identified. We are concerned that the security of the Department's IT systems may be compromised because of its inability to consistently and systemically mitigate identified security vulnerabilities. The Department recognizes this challenge and recently hired a contractor, who issued a report in July 2007, providing recommendations on how to improve its vulnerability management program, which would improve the security of its IT systems.

Vulnerability Identification

One of the first steps in securing an IT system is to identify its security vulnerabilities. The Department uses three methods to identify IT system security vulnerabilities: certification and accreditation (C&A), monthly IT system configuration scans, and audits and reviews.

Certification and Accreditation

Security certification is a comprehensive assessment of the management, operational, and technical security controls in an IT system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome to satisfy the security requirements for the IT system. In contrast, security accreditation is management's official decision to authorize the operation of an IT system. The Department's C&A process is documented in a C&A Handbook.[8]

Upon completion of the C&A process, the results and documentation of the C&A process and corrective plans of action and milestones (POA&M) created during the process are uploaded to CSAM, an IT system that automates the monitoring of FISMA compliance and vulnerability remediation.[9] Uploading the information to CSAM enables the Department to monitor its progress in meeting the President's Management Agenda and the components' progress in implementing the POA&Ms.[10] If the uploaded information shows any weaknesses in the system, the Information

[8] The C&A Handbook outlines the process, documentation requirements, and automated tools essential to performing a successful C&A of Department IT systems.

[9] POA&Ms are used to identify tasks that need to be accomplished, detailing the resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. The purpose of a POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.

[10] The President's Management Agenda requires that an agency maintains C&A for 100 percent of its IT systems.

Technology Security Staff (ITSS) in the Department's Office of the Chief Information Officer (OCIO) verifies that a POA&M was created and that the compensating control specified in the POA&M sufficiently mitigates the risk.

According to the Department's FY 2007 FISMA report to OMB, there are 225 systems in its IT inventory and all were accredited at the end of FY 2007. The certification and accreditation of each system gives the component's management, and ultimately the Department's management, assurance that the IT system will be placed into operation only after the component assesses security concerns and addresses any identified issues. Ultimately, the C&A process is designed to minimize the possibility of a security breach.

It is important to note that the C&A process occurs at a specific point in time and reflects a system's security control environment only at the time the C&A was conducted. Changes to the system, such as the addition of software, can affect the system's security as well as every system that connects to it. As a result, the C&A process must be coupled with continuous monitoring of a system's configurations. To this end, the Department instituted a monthly system configuration scanning process to identify vulnerabilities that may develop after the system completes the C&A process.

Monthly Configuration Scans

FISMA requires the Department to protect and secure its information systems by implementing appropriate tools that identify and validate system security configurations. To satisfy this requirement, the Department selected the Foundstone Enterprise (Foundstone) vulnerability management tool in 2004 to identify and validate system security configurations during vulnerability assessments. These assessments are performed as part of the monthly configuration scans. During the scanning process, each component uses Foundstone to electronically connect to all of its systems, including the hardware attached to those systems, and determine whether each system meets established baselines and configurations or if a vulnerability exists. If Foundstone identifies a vulnerability, the system and vulnerability is entered into CSAM and the Department monitors the remediation of the identified vulnerability.

The Department's vulnerability management plan requires each component to: (1) run Foundstone vulnerability scans on all networked electronic devices at least once every 30 days; (2) submit scan results to the ITSS for review and analysis; (3) assign responsibility, target dates, and monitor the progress for remediation of critical vulnerabilities identified

during the scans in POA&Ms; and (4) update CSAM to show the results of the scanning activities.[11] The ITSS is responsible for implementing the requirements of the vulnerability management plan within the Department. The ITSS reviews and evaluates the scan results to identify systemic vulnerabilities throughout the Department and ensure that identified vulnerabilities are addressed.

We reviewed the scan results for 6 months in FY 2007 for the 26 components whose vulnerability management programs the OCIO managed.[12] We found that these 26 components required by the OCIO to conduct monthly scans generally complied with the requirement. However, for the quarters ending March 31, 2007, and September 30, 2007, 7 of the 26 components did not submit scans.

The scan results we reviewed identified access control issues and [redacted] as systemic vulnerabilities within the Department's IT systems.[13] [redacted]

[redacted]

[11] ITSS selects and publishes a list of critical vulnerabilities in advance to ensure components can identify and remediate IT security vulnerabilities discovered during the monthly scans.

[12] Our analysis of the scan results included the fiscal year quarters ending March 31, 2007, and September 30, 2007.

[13] We were unable to determine how outdated the anti-virus software was because of the format in which the scan results were provided to us.

[14] An access control vulnerability is a system configuration that allows admission to a system or network resources that does not comply with the Department's system access requirements. An anti-virus vulnerability is outdated anti-virus software.

[redacted]

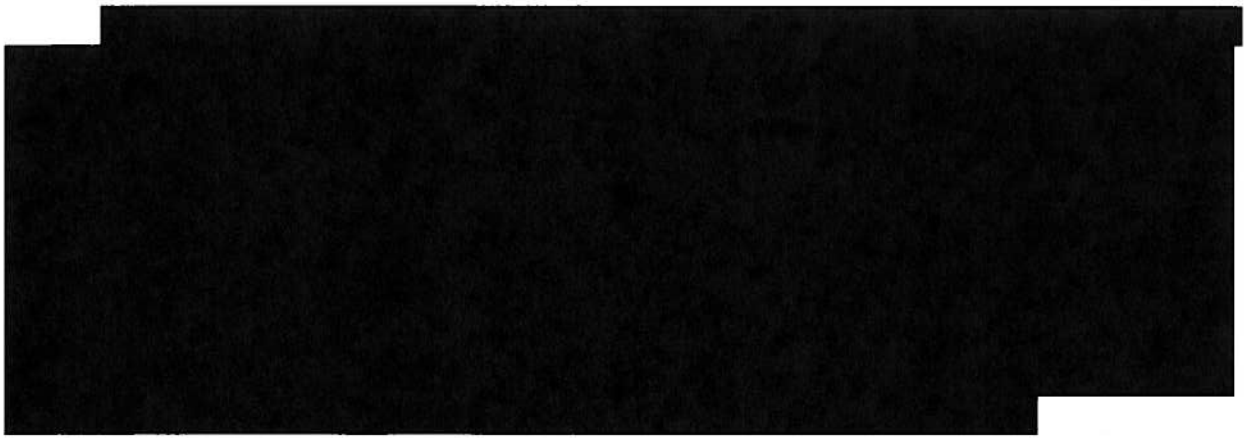
Prior Audits and Reviews

Several OIG and GAO reports provide additional information on the Department's IT security controls environment. Specifically, the annual FISMA and financial statement audits issued by the OIG identified access control issues as a Department-wide problem and also found that the components failed to apply global fixes to identified weaknesses, which contributed to the systemic nature of the vulnerabilities. In response to these reports, the Department created POA&Ms for all of the vulnerabilities identified by the OIG audits. Additionally, these POA&Ms are entered and tracked in CSAM until resolved. A more detailed discussion of these reports can be found in the "Prior OIG and GAO Reports" section of this report.

15 [redacted]

Vulnerability Remediation

A key element in implementing a vulnerability management program is following up on identified vulnerabilities to ensure that they are mitigated appropriately. We found that while the Department actively monitors the remediation of vulnerabilities identified during the C&A process and audits, it does not have an effective procedure for monitoring the remediation of vulnerabilities identified during the monthly scanning process.



The Assistant Director of the Enterprise Solutions Team of ITSS also noted that the National Institute of Standards and Technology (NIST) vulnerability assessment does not require remediation plans for identified

vulnerabilities, but only requires that the vulnerabilities be identified.[16] Therefore, to be FISMA-compliant a component does not have to show remediation plans for the vulnerabilities identified through the scanning process. Although the Department is ensuring that it meets FISMA requirements, it is still responsible for ensuring the security of the information contained within its IT systems, even if FISMA does not require a specific remediation step. We believe that a structured process for monitoring vulnerability remediation would improve the accuracy of the Department's assessment of the security controls environment of its IT systems.

The Department's Monitoring and Oversight

To ensure that its documented IT security program is implemented throughout its components, the Department has developed various monitoring and oversight procedures including the Information Technology Security Council (ITSC), the POA&M process, the OCIO reviews, and the ITSC Program Progress Report Card (Dashboard).

Information Technology Security Council

The ITSC is the central focal point of the Department's IT Security Program. The ITSC is a collaborative team that manages the Department's IT security priorities and compliance with government policies and regulations. A review conducted by an independent contractor, Deloitte and Touche, LLP, in July 2007 found that the lack of accountability and authority to implement and enforce security initiatives could result in ineffective risk management and lack of assurance for the protection of critical assets. According to the Deputy Director of ITSS, the Department is in the process of restructuring the ITSC as proposed by the independent contractor's report.

Plans of Action and Milestones

The Department's IT Security Program Management Plan requires that the ITSS annually review all POA&Ms that are uploaded into CSAM, although the review is limited to POA&Ms created for vulnerabilities identified during C&A process and audits and reviews. The plan does not require, and the ITSS does not perform, an annual review of the component's remediation

[16] NIST is responsible for developing standards and guidelines for providing adequate information security for all agency operations and assets. FISMA required NIST to develop technical guidance for conducting vulnerability assessment. The OIG uses NIST guidance to review the Department's compliance with the FISMA requirements.

plans for addressing vulnerabilities identified during the monthly system scans.

The Assistant Director of the Enterprise Solutions Team of ITSS stated that the Department monitored the remediation of known security vulnerabilities by examining the number of vulnerabilities identified by the monthly scans. For example, if a component's monthly scan identified 100 vulnerabilities in July and 90 in August, the Department would assume that the component was actively addressing the vulnerabilities. Conversely, if the number of vulnerabilities increased, the Department would assume that the component was not aggressively working to eliminate identified vulnerabilities in its IT systems.

In our judgment, this approach fails to consider the removal or addition of systems to a component's IT environment. Although each Department component is responsible for scanning all systems in its inventory, the Department has no way of monitoring whether each component is actually scanning all of its systems. As a result, a component could exclude some systems from the monthly system scan to lower the number of vulnerabilities reported without the Department's knowledge. We believe that a month-to-month comparison of a component's total number of vulnerabilities is an ineffective way of monitoring the remediation of identified vulnerabilities. Additionally, we recommend that the Department maintain an inventory list of all its networked system devices and use the list to confirm that the components are conducting monthly scans of all of their systems.

OMB requires agencies to prepare and submit quarterly updates to POA&Ms. These updates should address all vulnerabilities identified during the annual FISMA review, as well as those vulnerabilities identified during other reviews, such as vulnerability assessments, which include monthly system scans. The Department's rescission of the POA&M requirement for vulnerabilities identified during the monthly scanning process not only eliminates a structured process for monitoring known critical vulnerabilities, but also violates the OMB requirements for quarterly POA&M updates. As a result, the Department's quarterly POA&M updates to OMB may be incomplete and inaccurate.

Office of the Chief Information Officer Reviews

The ITSS reviews C&A documentation, documentation supporting the component's successful implementation of a control, and POA&Ms to determine compliance with applicable guidelines. The ITSS details the results of the reviews in the CSAM tool kit. To ensure that previously

established POA&Ms meet the requirements of the Department and OMB, OCIO reviewers examine all system POA&Ms in CSAM.

It is important to note that the POA&Ms examined by OCIO reviewers are those resulting from C&A activity that does not include monthly scanning for vulnerabilities. The components are responsible for tracking the remediation of vulnerabilities identified from the monthly scans, which are not recorded in CSAM. However, since the monthly scan information is not recorded in CSAM, the ITSS is not reviewing the status of related vulnerability remediation during the OCIO annual review.

Dashboard

A "Dashboard" on IT security is prepared for all Department components that develop or operate IT systems. The Department uses a three-color (red, yellow, green) methodology on its Dashboard to grade the components' compliance in areas such as risk assessment, C&A, POA&M completion, vulnerability assessments, and incident response. The graded criteria for each project area differ based on the Department's requirements for that project area.

During our review, we noted that the scoring methodology only takes into consideration that the monthly scans were completed, not the status of actions taken to address the identified vulnerabilities. As a result, a component could receive a green rating for vulnerability assessment without doing anything to improve the security of its IT systems. While the Dashboard rating methodology may be effective in tracking the Department's progress towards FISMA compliance, it does not provide an accurate and clear status of the Department's overall IT security environment. We believe the Department should go beyond compliance testing and validation to ensure that its IT systems and information resources are properly secured.

Future of the Department's Vulnerability Management Program

During our audit, the Department was taking steps to overhaul its vulnerability management program. The Department hired a contractor who issued a report in July 2007 providing recommendations on how to effectively revamp the vulnerability management program. Also, at the time of our audit the Department was in the process of establishing the Justice Security Operations Center (JSOC) to better manage its vulnerability

management program.[17] The Department intended to implement JSOC through an iterative approach of adding components and services to reach final operating capability with full implementation around the fourth quarter of FY 2009. The Department spent $1.1 million in FY 2007 and budgeted $600,000 in FY 2008 for the implementation of JSOC. At the time of our audit, the Department had not yet determined the total cost to fully implement JSOC.

The core technology for the success of JSOC is [redacted], a software tool that will identify systemic vulnerabilities on all Department systems that are linked to [redacted]. For example, if outdated anti-virus software is detected on a system, [redacted] will be able to search for other systems on the network also using the outdated software. Even with the use of [redacted], however, the Department will require that monthly scans continue to be performed. With [redacted], system analysts will not be required to manually analyze the monthly scans. Instead, the Department would link Foundstone with [redacted] so that after components complete the monthly scans, scan results would be entered into [redacted] that would combine the data, thus allowing for easier data analysis.

[redacted]

Conclusion and Recommendations

We found that the Department has well-documented processes and procedures for its vulnerability management program. However, mitigating identified vulnerabilities continues to be a concern. During our audit, we

[17] JSOC will provide the Department with real-time monitoring of security and network health by proactively identifying security incidents, facilitating incident responses, and providing security information to help management make risk-based decisions.

[18] [redacted]

found that the Department was monitoring the resolution of vulnerabilities identified during the C&A process. However, it did not monitor all vulnerabilities identified during the monthly configuration scans. The Department contends that the resolution of these vulnerabilities was not required to meet the requirements of NIST. Nevertheless, the lack of a monitoring system to ensure that these vulnerabilities are resolved can place the Department's IT systems at risk.

The Department recognized the deficiencies in its vulnerability management program and hired an independent contractor to provide recommendations on how to improve the management of identified vulnerabilities. In addition, the Department is establishing JSOC to provide a more comprehensive, real-time approach to information analysis and vulnerability remediation. Yet, until the contractor completes its report, the recommendations are implemented, and JSOC is fully operational, the Department's ability to monitor and ensure that its IT systems and the information contained in them are reasonably secured is significantly diminished.

This audit report contains four recommendations that address the Department's management of its information systems program. For example, we recommend that the Department's CIO should establish a mechanism for monitoring remediation of all identified IT system vulnerabilities, as well as a methodology that ensures global fixes are made for known vulnerabilities. The Department should also conduct and maintain an inventory of all IT devices that communicate on the Department's networks.

TABLE OF CONTENTS

INTRODUCTION

Mirroring society at large, the federal government and the Department of Justice (Department) have become increasingly dependent on information technology (IT) systems to accomplish its mission. These systems are used to gather, maintain, and utilize a wealth of data regarding individuals, organizations, nations, and a wide range of other oftentimes sensitive information. A significant risk involved with relying on IT systems is that they contain flaws or omissions in their design or the means in which they are implemented. These flaws and omissions are commonly referred to as vulnerabilities. If exploited, vulnerabilities in IT systems can expose sensitive information to unauthorized individuals and in some cases compromise our national security.

Eliminating all vulnerabilities from all IT systems is not possible because IT systems are constantly changing with the introduction of new software or hardware, and these changes introduce the possibility of additional vulnerabilities. To reduce the risk of harm to its IT systems or the data they contain, however, it is essential that the federal government manage the vulnerabilities identified in its IT systems. Managing those vulnerabilities and enhancing the security of the information contained in federal IT systems is a top priority of the federal government, including the Department.

Federal Information Security Management Act of 2002

The *Federal Information Security Act of 2002* (FISMA) was enacted by Congress and signed into law by the President as *Title III of the E-Government Act of 2002*. FISMA assigns specific responsibilities to the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB) in order to strengthen information system security in the federal government. NIST is responsible for developing and issuing standards, guidelines, and other publications to assist federal agencies in implementing FISMA requirements and managing cost-effective programs to protect their information and information systems. OMB is responsible for overseeing and enforcing accountability for agency compliance with the FISMA requirements.

In addition, FISMA requires the head of each federal agency to implement policies and procedures to reduce IT security risks to an acceptable level and in a cost-effective manner. FISMA also requires federal agencies to develop, document, and implement information security programs that support the operations and assets of the agency. According

to NIST, the following are part of this broad requirement for an effective information security program:

- periodic assessments of risks and the magnitude of harm that could result if the risks are realized;

- periodic testing and evaluation of the effectiveness of information security procedures, practices, and policies; and

- processes for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in information security policies, procedures, and practices of the agency;

In June 2003, the Department's Chief Information Officer (CIO) appointed a Chief Information Security Officer (CISO) to support the implementation of FISMA and to provide leadership for the Department's IT Security Program.

Department of Justice's IT Security Program

The Department's IT Security Program includes periodic assessments of risk, including the potential harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. The security program also includes periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls to be performed at least annually or more frequently depending on risk.

Risk management is a major component of the Department's IT Security Program. As part of the system development life cycle (SDLC) process, the Department requires components to conduct risk assessments for systems undergoing development or major modifications.[19] The SDLC process also helps to identify appropriate controls for reducing or eliminating risk early in a system's development. Further, the Department has developed a risk assessment methodology that describes the steps required

[19] The SDLC is a planning document used by the Department to establish standardized procedures, practices, and guidelines governing the initiation, concept development, planning, requirement analysis, design, development, integration and testing, implementation and operations, maintenance, and disposition of information systems within the Department.

to produce an information security Risk Assessment Results report.[20] This report is incorporated into the system security plan (SSP) and is reviewed during the security certification and accreditation (C&A) process.[21]

Security certification is a comprehensive assessment of the management, operational, and technical security controls in an IT system to determine the extent to which the controls are meeting the security requirements for the IT system. Security accreditation, on the other hand, is management's official decision to authorize the operation of an IT system. By authorizing the operation of a system, management explicitly accepts the risk to Department and component operations, assets, or individuals based on the implementation of an established set of IT security controls.

The Department has also developed a Vulnerability Management Plan designed to provide guidance to its security and operations personnel for identifying and mitigating risks within the IT environment.[22]

Security awareness training is also included within the Department's security program. This training is designed to inform Department personnel of the information security risks associated with their activities and their responsibilities in complying with Department policies and procedures designed to reduce those risks. The Computer Security Awareness Training is a Department-wide, web-based course that provides awareness training to all Department employees and contractors. IT professionals with IT security functions are also required to complete training according to the level of their positions (beginner, intermediate, and expert). They must also complete technical training based on their specific IT functions within the Department.

---

[20] The Risk Assessment Results report describes each of the information system's major risks, the recommended countermeasures to mitigate each of those risks, and the cost and schedule for implementing all risk mitigation. The report serves as the statement of residual risk in a component's system security plan (SSP).

[21] The SSP identifies the current security environment, establishes scope and objectives, and outlines the activities required for security implementation. It also describes the system's security requirements, the controls in place or planned, and the roles and responsibilities of all authorized individuals who use the system.

[22] The document is entitled "Foundstone Vulnerability Management Compliance and Validation, Version 2," March 9, 2007. The Department uses Foundstone Enterprise (Foundstone) to administer the vulnerability management plan. Foundstone is a vulnerability software package distributed by McAfee Security Services that identifies security vulnerabilities and assigns risk factors based on the extent of possible harm that could be caused if the vulnerabilities were exploited.

Information Technology Security Council

To manage and implement its IT security program, the Department's CIO established the Information Technology Security Council (ITSC) in August 2003. The primary objective of the ITSC is to provide comprehensive, Department-wide IT security program management, which includes ensuring the Department's IT security policies, programs, and processes are managed in compliance with existing Department and federal policies. The Department's Deputy Chief Information Officer chairs the ITSC, and each Department component has a member on the council.

IT Security Program Management Plan

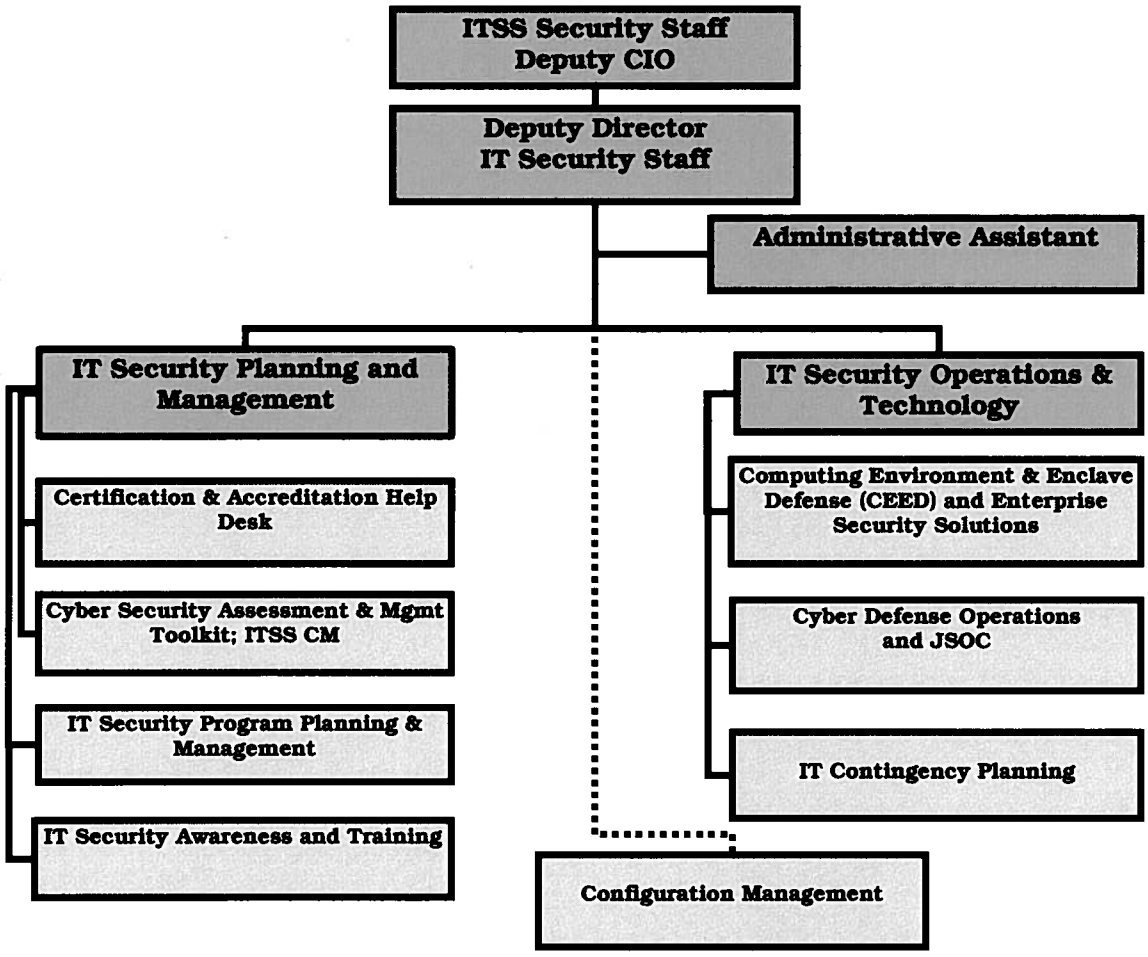
In fiscal year (FY) 2004, as one of its first actions the ITSC developed an initial IT Security Program Management Plan. This plan established the Department's efforts to secure its major applications, general support systems, and the information processed on those systems. The plan is updated regularly to ensure that the plan addresses newly recognized security issues.

Information Technology Security Staff

The Department's Information Technology Security Staff (ITSS) is responsible for implementing the requirements of the IT Security Program Management Plan within the Department. The ITSS mission is to ensure the protection of the Department's information systems that collect, process, transmit, store, or disseminate either classified or sensitive but unclassified information. To accomplish its mission, the ITSS is responsible for performing a wide variety of functions, including the development and implementation of Department-wide IT standards, procedures, and guidelines governing the security of Department classified and sensitive but unclassified information systems.

The ITSS is organized into six project teams. An ITSS staff member chairs each team, which is composed of members from various Department components. The teams are: (1) certification and accreditation (C&A), (2) computing environment and enclave defense, (3) configuration management, (4) Department Computer Emergency Readiness Team/Cyber Defense Operations (CDO), (5) IT contingency planning, and (6) IT security employee services. The following chart shows the organizational structure of the ITSS.

ITSS Organization



Source: OCIO Information Technology Security Staff

Prior OIG and GAO Reports

The Department of Justice Office of the Inspector General (OIG) has previously conducted inspection reviews, financial statement audits, and FISMA audits examining the Department's IT security. In addition, the Government Accountability Office (GAO) issued a report on agency needs to address challenges in implementing IT statutory requirements, and the Department was included within that report. These reports are discussed below.

OIG Reviews

The OIG conducted a review of the *Department of Justice's Reporting Procedures for Loss of Sensitive Electronic Information*, issued in June 2007, which identified deficiencies in the Federal Bureau of Investigation's (FBI) compliance with reporting procedures for loss of sensitive data. Specifically, the FBI did not report all incidents involving the loss of electronic devices to the Department's Computer Emergency Readiness Team or all incidents involving classified information to the Department's Security and Emergency Planning Staff. The audit also found indications that most of the Department components were not consistently reporting computer security incidents, such as loss of equipment containing personally identifiable information, in a timely manner. The OIG made eight recommendations related to computer security incident reporting.

Financial Statement Audit Reports

Under the direction of the OIG, independent public accountants perform the annual financial statement audits of the Department and its components. These financial statement audits include a review of the IT general control environments that support the financial systems used to process financial information. The IT general controls reviews are performed based on the GAO's *Federal Information System Controls Audit Manual (FISCAM)* and NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*. FISCAM provides a methodology for evaluating the internal controls over the integrity, confidentiality, and availability of data within IT systems.

The Department received an unqualified opinion on its FY 2007 consolidated financial statements, with two significant deficiencies, compared to one material weakness and one reportable condition for FY 2006. Both of the Department's significant deficiencies were repeat weaknesses in the general and application controls for each of the

Department's component financial systems. The FBI's deficiencies in general and application controls were considered a material weakness.

The FY 2007 consolidated financial statement audit report stated that while the Department's financial statement audit results continued to improve, the Department still lacked sufficient automated systems to readily support ongoing accounting operations and financial statement preparation. Inadequate, outdated, and in some cases non-integrated financial management systems did not provide certain automated financial transaction processing activities necessary to support management's need for timely and accurate financial information throughout the year. Many tasks must be performed manually at interim periods and at year's end, requiring extensive manual efforts on the part of financial and audit personnel. The report stated that these significant, costly, and time-intensive manual efforts will continue to be necessary for the Department and its components to produce financial statements until automated, integrated processes and systems are implemented that readily produce the necessary information throughout the year. The report added that while the Department is proceeding towards a Unified Financial Management System (UFMS) that it believes will correct many of these issues, implementation has been slow and will not be completed across the Department for at least another 5 years.

FISMA Audit Reports

Under the direction of the OIG, independent auditors performed FY 2007 FISMA reviews of the security programs of four Department components and reviewed four sensitive but unclassified systems. These reviews found that the Department had ensured that systems within the four components reviewed were certified and accredited, system security controls were tested and evaluated within the past year, and system contingency plans were tested in accordance with FISMA policy and guidance. The OIG also reviewed documented policies and procedures for reporting incidents internally to the United States Computer Emergency Readiness Team (US-CERT), which was established in 2003 to coordinate the defense against and responses to cyber attacks. Our review found that three of the four components followed documented policies and procedures for reporting incidents internally. However, the fourth component did not report such incidents in a timely manner.

GAO Report

The GAO's August 2007 Information Security Report addressed selected agencies' need to focus on challenges in implementing IT-related statutory requirements.[23] The report stated that the Department of Justice faced challenges in implementing key information security control activities required by FISMA and OMB. Specifically, the report identified weaknesses relating to the Department enforcing system configuration policies, testing and evaluating controls, and remedial actions. The GAO recommended that the Department's CIO:

- develop and implement Plans of Action and Milestones (POA&Ms) to achieve full implementation of common security configurations across all system platforms;
- address the weaknesses in security control testing policies as described in the report; and
- reconcile redundancies in the department's remediation plan tracking tool.

[23] U.S. Government Accountability Office, *Information Technology: Selected Departments Need to Address Challenges in Implementing Statutory Requirements*, GAO-07-528 (August 2007) 23 – 25.

FINDING AND RECOMMENDATIONS

The Department has appropriately documented the processes and procedures necessary for managing its vulnerability management program and implementing the established practices for identifying known vulnerabilities. This positive performance resulted in the Department receiving an A^+ grade on its 2007 FISMA report card issued by the House Committee on Oversight and Government Reform. However, we concluded that, notwithstanding the positive record in documenting these procedures, the Department needs to focus more on mitigating the identified vulnerabilities. Our review identified major systemic security vulnerabilities in Department IT systems, such as inadequate access controls, outdated anti-virus software, and outdated patches. Yet, in FY 2007 the Department changed its requirements for the remediation of vulnerabilities identified during monthly scans of its IT systems that limits the Department's ability to improve the security of its information. While the Department may satisfy FISMA requirements with this change, it does not adequately ensure security in the Department's IT systems. In addition, we found that the Department does not have an accurate inventory of all Department-wide networked devices, and without this information is unable to adequately assess whether the Department's systems are truly secure.

IT Vulnerability Management

IT vulnerability management includes the identification and remediation of known vulnerabilities. The Department's vulnerability management program is an essential part of the continuous monitoring activities within its IT security program.[24] The purpose of continuous monitoring is to provide oversight and review of IT security controls on an ongoing basis. The Department's vulnerability management plan communicates requirements for vulnerability scanning, reporting, and compliance validation to security and operations personnel throughout the Department.

[24] Vulnerability management is a process designed to eliminate or mitigate system vulnerabilities and sustain compliance based on risk and cost.

The Department has also implemented the Cyber Security Assessment and Management (CSAM) automated tool kit to manage the implementation of the vulnerability management plan requirements and to meet the FISMA reporting requirements.[25]

Vulnerability Identification

The Department's IT Security Program Management Plan documents the three methods used to identify system vulnerabilities: the C&A process, monthly IT system configuration scans, and independent audits and reviews.

Certification and Accreditation

The Department has documented its C&A process in a C&A Handbook.[26] According to the Handbook, all Department IT systems should be accredited prior to being placed into operation. For new IT systems or major upgrades to IT systems, C&A activities begin early in the SDLC process (during the initiation phase) and continue through to the disposition phase.[27] For operational IT systems and older legacy IT systems, the C&A activities may, by necessity, begin later in the SDLC process (during the operations and maintenance phases). The primary document produced as a result of the C&A process is the System Security Plan (SSP).[28]

In its August 2007 report, GAO stated that for FY 2006 the Department had achieved success in its C&A activities. According to the report, 100 percent of the Department's systems were certified and

---

[25] CSAM is the Department's FISMA compliance, management, and automated reporting tool, which provides five services: (1) risk-based policy and implementation guidance, (2) enterprise program management plan, (3) system security plan and implementation, (4) management reporting, and (5) training. CSAM is used to monitor the remediation of identified system vulnerabilities.

[26] The C&A Handbook outlines the process, documentation requirements, and automated tools essential to performing a successful C&A of Department IT systems.

[27] An IT system's SDLC has five phases: initiation, development or acquisition, implementation, operation or maintenance, and disposal.

[28] The SSP also provides guidelines to establish system security and privacy requirements. It identifies the current security environment, establishes scope and objectives of the system, and outlines the activities required for security implementation. It also describes the system's security requirements, the controls in place or planned, and the roles and responsibilities of all authorized individuals who use the system.

accredited and the processes governing the C&A activities were good. The Department met its goal of maintaining the same level of efficiency in its C&A activities for FY 2007. According to the Department's FY 2007 FISMA report to OMB, all of the 225 systems in the Department's inventory were accredited by the end of FY 2007.

In CSAM, a system with a current authority to operate is considered to have successfully completed the C&A process. An IT system's failure to receive such authority usually indicates that there are major deficiencies in the IT security controls or that the component has failed to update the existing authority to operate. In our opinion, the absence of proper accreditation for some systems can make the component's IT systems, and in some cases the entire Department's IT systems, vulnerable to potential threats. For example, if one of the non-C&A systems is connected to the Department-wide network, that system exposes the other systems on the network, whether accredited or not, to potential threats.

It is important to note that the C&A process occurs at a specific point in time and only reflects a system's security control environment at the time the C&A was conducted. Changes to the system, such as the addition of software, can affect the system's security as well as every system that connects to it. As a result, we believe the C&A process must be coupled with the continuous monitoring of a system's configurations. The Department instituted a monthly system configuration scanning process to identify vulnerabilities that may develop after the system goes through the C&A process.

Monthly Configuration Scans

The monthly configuration scanning process is designed to identify vulnerabilities and provide the Department with a status of its IT system security. The VM Plan requires all components to: (1) run the Foundstone Enterprise (Foundstone) vulnerability management tool and scan all networked electronic devices at least once every 30 days; (2) submit scan results to the ITSS for review and analysis; (3) assign responsibility, target dates, and monitor the progress for remediation of critical vulnerabilities identified during the scans; and (4) update CSAM with the results of the scanning activities.[29] The ITSS reviews the scan results to identify systemic vulnerabilities throughout the Department and updates the ITSC Program Progress Report Card (Dashboard). The Dashboard is a monitoring

[29] ITSS selects and publishes a list of critical vulnerabilities in advance to ensure components can identify and remediate IT security vulnerabilities discovered during the monthly scans.

mechanism used by the Department to visually present components' compliance with vulnerability assessment policies.

A component's non-compliance with the Department's system scanning requirement places its own IT information at risk to potential threats because the lack of scanning can make it difficult to identify and mitigate vulnerabilities in the system. It also jeopardizes the information contained in other systems throughout the Department that are connected to the component's system.

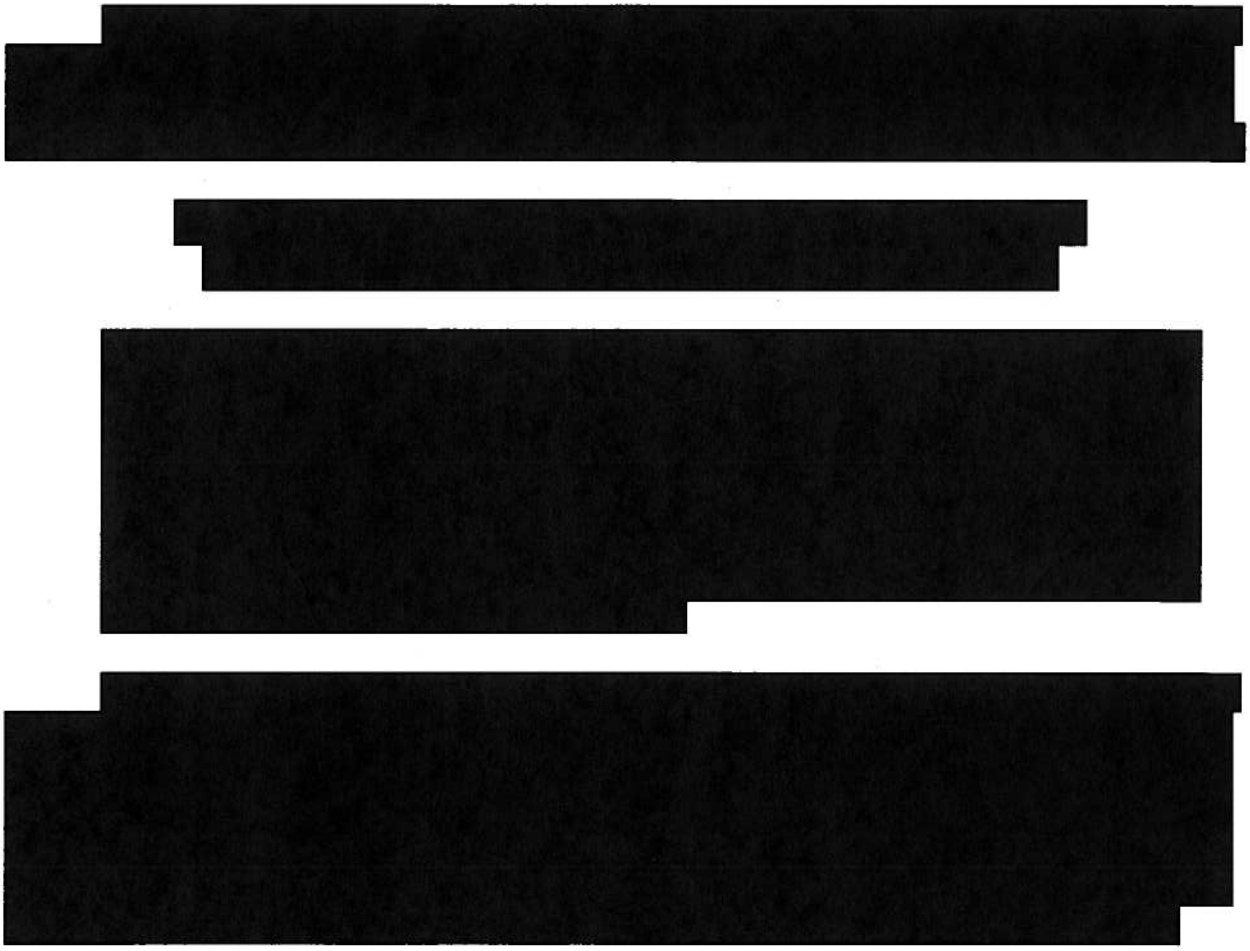
---

[30] The sample components included the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), Federal Bureau of Prisons (BOP), Criminal Division, Drug Enforcement Administration (DEA), Executive Office for Immigration Review, Executive Office for United States Attorneys (EOUSA), Executive Office for United States Trustees, FBI, Office of Justice Programs (OJP), and U.S. Marshals Service (USMS).

[31] The other five components were not a part of our sample; as a result, we did not interview personnel from those offices.

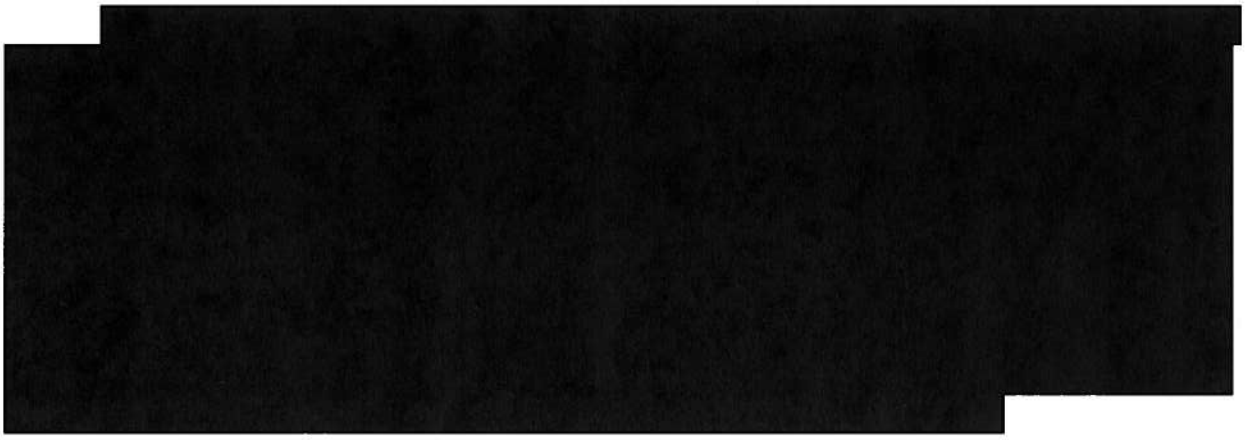
Systemic Vulnerabilities

The Department's CISO stated that access controls and outdated security patch vulnerabilities appear to be systemic throughout the Department. We analyzed the monthly system scans to determine whether access controls and outdated security patch vulnerabilities were systemic and if the Department may have overlooked other vulnerabilities that could be systemic throughout the Department.



Our analysis of the scan results showed that access control and outdated anti-virus software vulnerabilities are systemic throughout the Department. The scans did not identify outdated security patches as a systemic problem. However, we included outdated security patches in our analysis because of the Department CISO's concern with the components' inability to successfully implement security patches as required by the Department's VM Plan.

Access Controls. Access controls refer to the policies, procedures, and practices that govern the identification and authentication of a person gaining access to and operating an IT system. Identification and authentication are used to verify the identity of the user. This can be done by using passwords, personal identification numbers, smartcards, or tokens. Generally, the Department uses passwords to authenticate users and grant access to its IT systems.



[redacted]

[redacted]

[redacted]

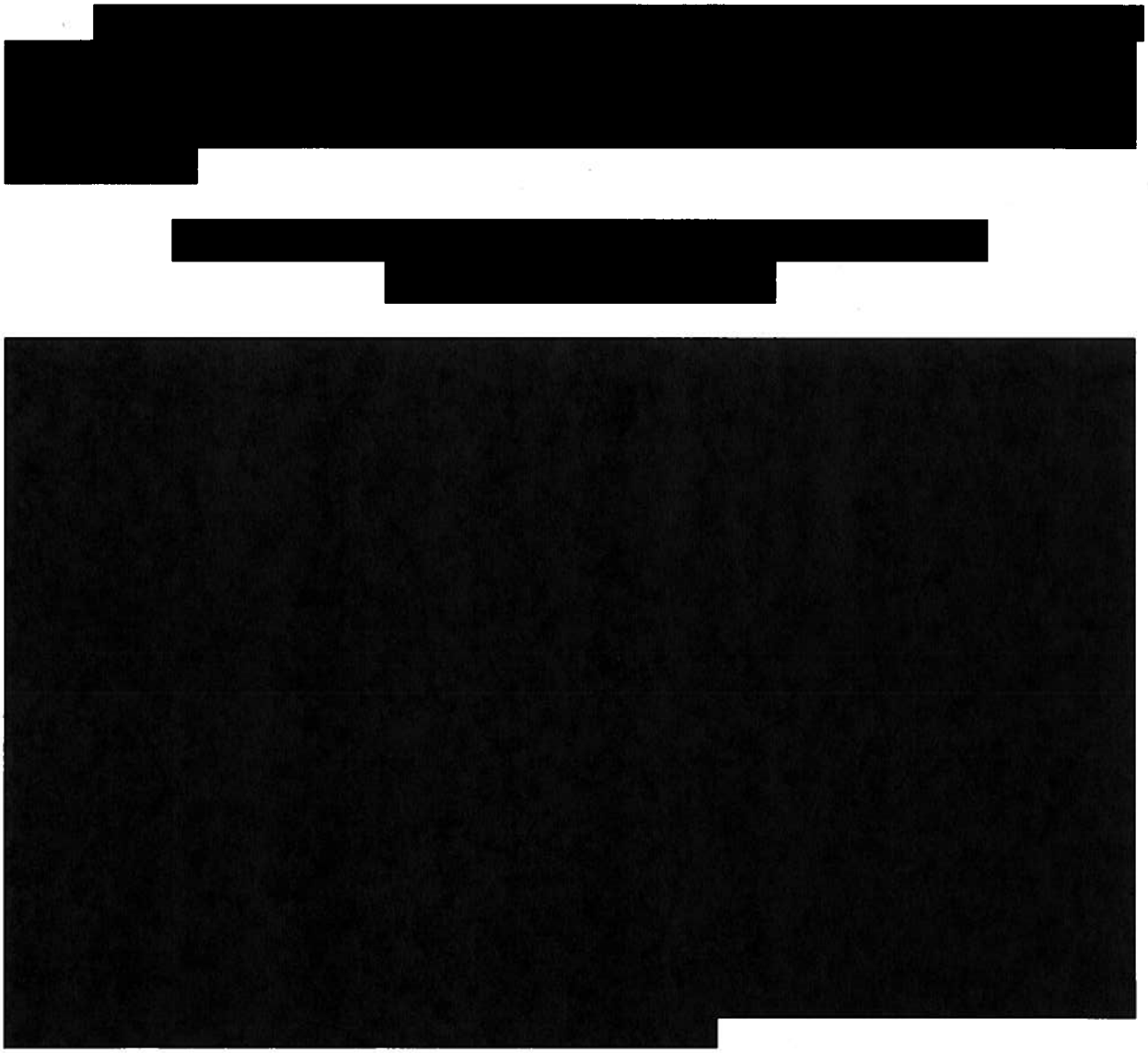
Outdated Anti-virus Software. Anti-virus software refers to one program or a collection of programs meant to protect a computer system

[redacted]

[redacted]

[redacted]

from computer viruses. Viruses are software programs that are designed to spread from one computer to another and interfere with the computer's operation. Anti-virus software is used to find, remove, or fix files that are infected with computer viruses. The main element of the anti-virus software is the scanning engine. Viruses created by hackers and cyber criminals can spread via infected e-mail attachments, shared files, or malicious websites. The anti-virus software scans the files or a computer's memory for certain patterns that may indicate an infection. The patterns it looks for are based on the signatures or definitions of known viruses. If it finds a virus, the application informs the user and cleans, deletes, or quarantines any files, directories, or disks affected by the malicious code.



Although some viruses are not harmful, many are meant to destroy information stored on the computer, make computers inoperable, or install backdoor programs that allow virus writers to remotely take control of a computer. Virus programs frequently exploit e-mail and web browser programs opened by unsuspecting users, and new and updated viruses are constantly being released. Because of the dangers that viruses present, if anti-virus software is not updated with the latest definitions to detect the newly identified viruses and if a system or network is infected, the virus can be transmitted between computers on a network, causing widespread loss of user data and software and potentially immobilizing an entire network. The Department must aggressively monitor the remediation of the identified vulnerabilities on a more global scale to ensure they do not compromise the Department's IT systems and information.

Outdated Security Patches. The objective of the vulnerability management plan is to ensure that all information systems and networks are configured with sufficient security to protect their information, and the systems are updated and patched to eliminate known vulnerabilities. Patch management involves acquiring, testing, and installing multiple fixes or code changes for known system vulnerabilities. According to an industry report, patch management is difficult because there are too many patches that must be installed and not enough time to ensure that they are installed. This issue is exacerbated because exploitation of the vulnerabilities can occur faster than patches are created.[34]

If security patches are not installed in a timely manner, the consequences can be serious. For example, an unauthorized user (hacker) can exploit an un-patched vulnerability and gain access to an entire IT system. The hacker can use this access to retrieve authorized usernames and passwords. This information can subsequently be used to obtain additional account information that allows the hacker to escalate standard user account privileges to administrator account privileges, which gives the hacker full control of the system.

In other cases, a system may be vulnerable to a denial of service attack, preventing authorized users from working.[35] Although a denial of service attack does not usually result in the theft of information or other

---

[34] See, e.g., John Fontana, "How to Handle Patch Management," *Network World*, December 1, 2003, http://www.networkworld.com/research/2003/1201howtopatch.html (accessed on January 28, 2008).

[35] A denial of service attack is an attempt to make computer resources and services unavailable to legitimate users.

security loss, it can disrupt the systems of the target. Typically, the result is the unavailability of a particular network service, such as e-mail. [redacted]

The Department's Chief IT Security Technologist stated that the Department has not created a formal document describing the Department's patch management policy. Rather, the Department developed and uses the following System and Technology Integrity (SI) standards as guidance for implementing patches;

- SI-02-01-01- The organization identifies information systems affected by recently announced software flaws and potential vulnerabilities resulting from those flaws; installs newly released security relevant patches, service packs, and hot fixes on the information system in a reasonable timeframe in accordance with organizational policy and procedures; and tests information system patches, service packs, and hot fixes for effectiveness and potential side effects before installation.

- SI-02-04-01- The organization conducts continuous security assessments to identify vulnerabilities in the information system within its operating environment; tests information system patches, service packs, and hot fixes for effectiveness and potential side effects before installation; and captures all appropriate information pertaining to the discovered flaws, including the cause of the information system flaws, mitigation activities, and lessons learned to identify necessary improvements in the flaw remediation process.

- SI-02-07-01- The organization centrally manages the flaw remediation process for information systems and employs a centralized patch management program to assist system administrators in identifying, acquiring, testing, and deploying patches.

- SI-02-08-01- The organization's security flaw remediation capabilities are effective and security flaw remediation actions have been performed on the information system.[36]

[redacted]

[redacted]

According to the Department's Chief IT Security Technologist, the Department expects patch management to be a part of the Justice Security Operations Center (JSOC) initiative. The JSOC initiative will provide the Department with real-time monitoring of security and network health by proactively identifying security incidents, facilitating incident responses, and providing security information to help management make risk-based decisions. The Department's Chief IT Security Technologist also stated that the JSOC will also give the Department the ability to perform global roll-outs of security patches to all affected systems Department-wide.

The OIG's annual FISMA audits found that the components' inability to apply global fixes to identified weaknesses contributed to the systemic nature of certain systems' vulnerabilities. [redacted]

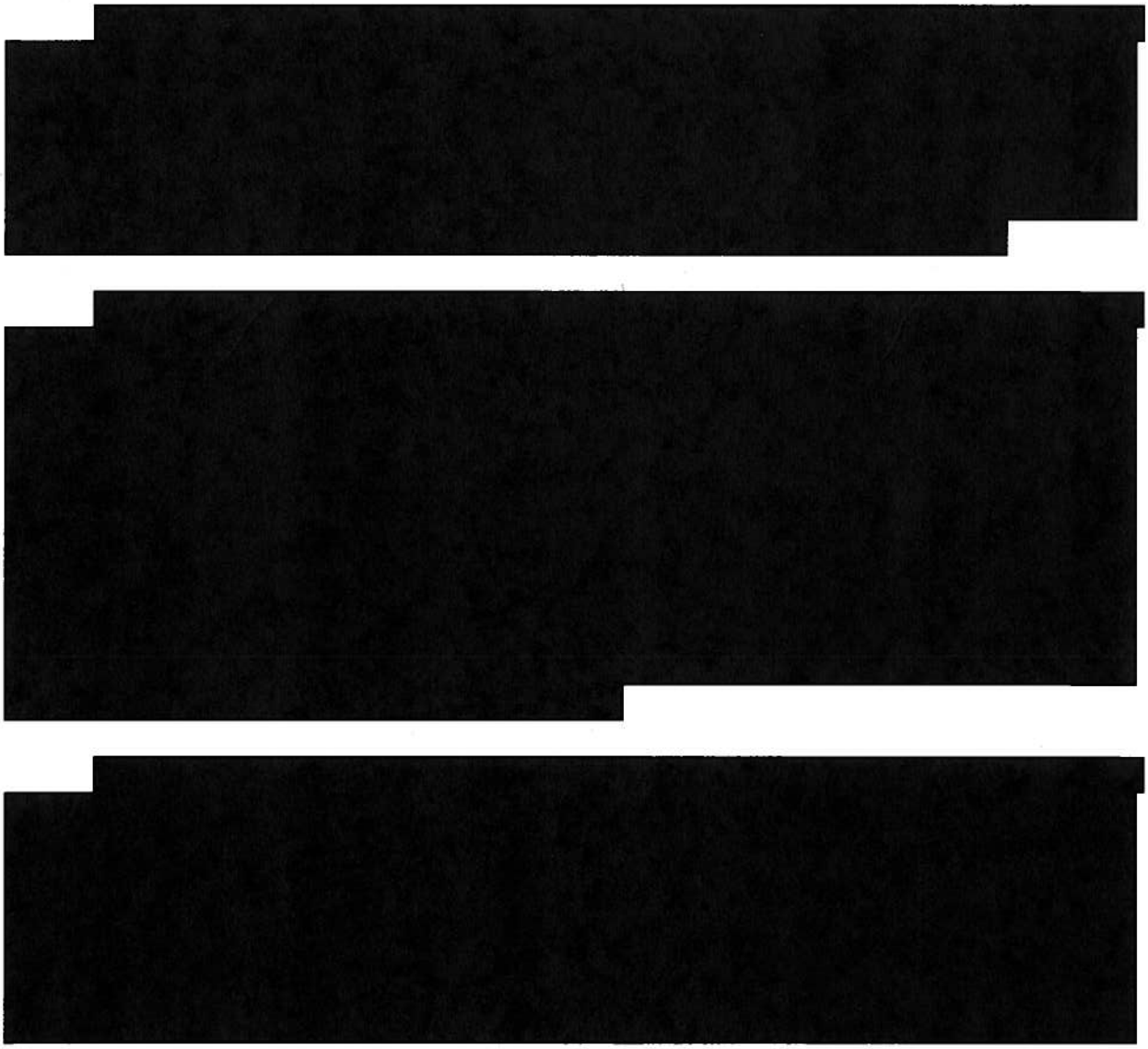
When asked why access controls and outdated anti-virus software issues remain problematic, the Department's CISO stated that a fluid IT

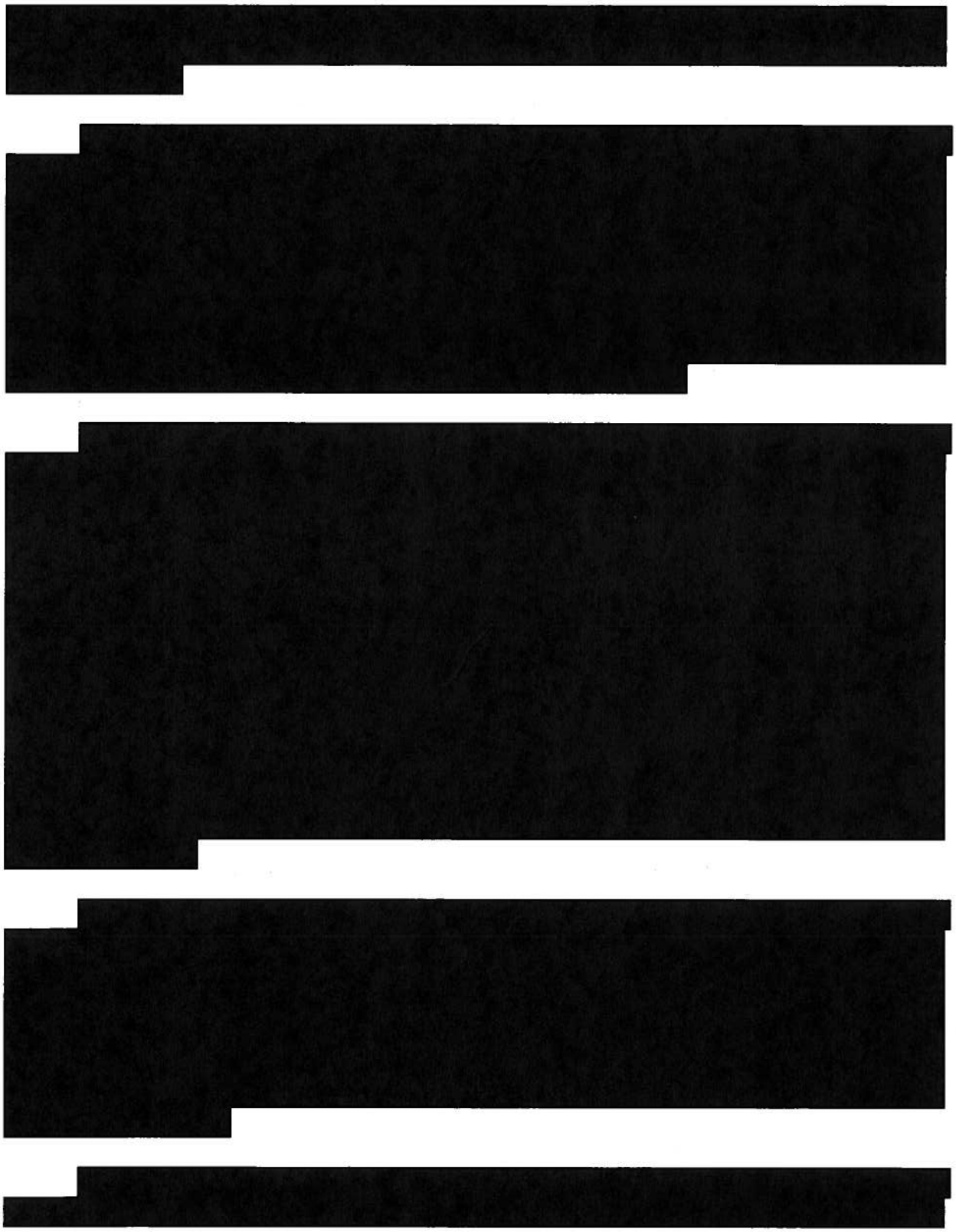
[36] The document is entitled Department of Justice Information Technology Security Standard, System and Information Integrity Control Family, Version 2.0, December 2006.

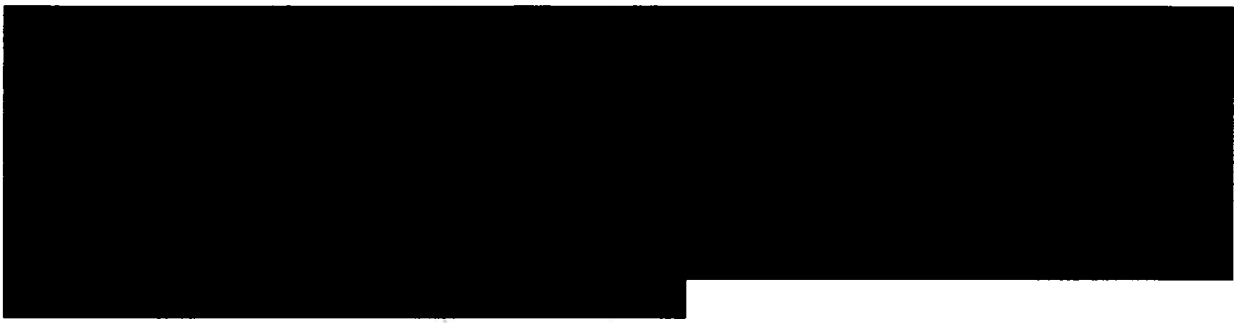
security environment contributes to the systemic nature of these issues. He noted that information systems technology is constantly changing. New computers and software updates are installed, existing computers are changed to include new software, and vendors are issuing fixes for known threats and vulnerabilities.

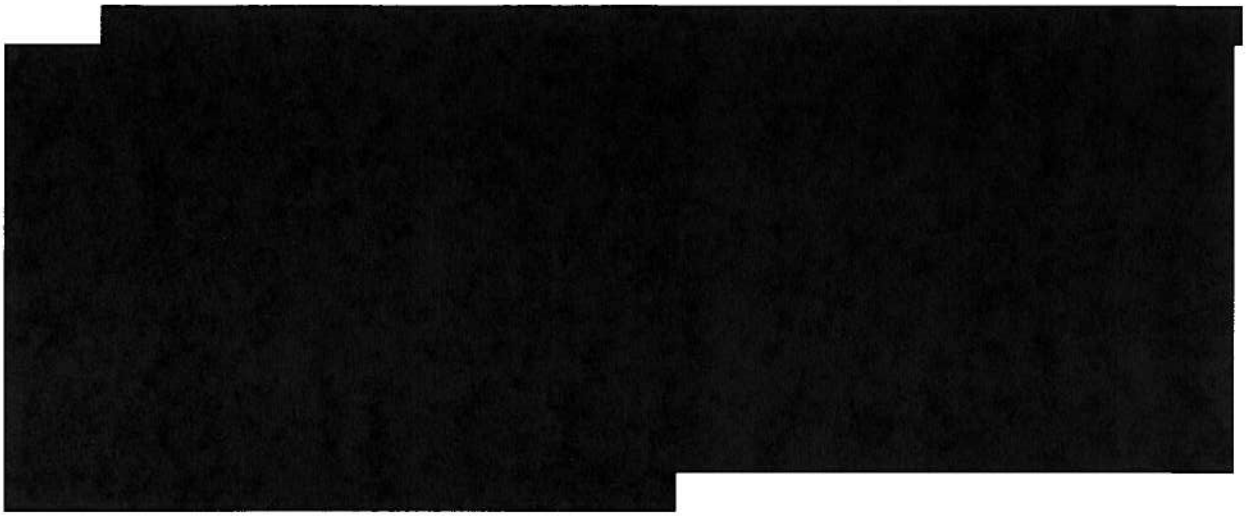
We agree that the nature of IT security is constantly changing. Because of the fluid nature of IT security overall, we believe the Department must continue to aggressively monitor the remediation of the identified vulnerabilities on a more global scale to ensure that frequent changes in IT systems do not compromise the Department's IT systems and information.

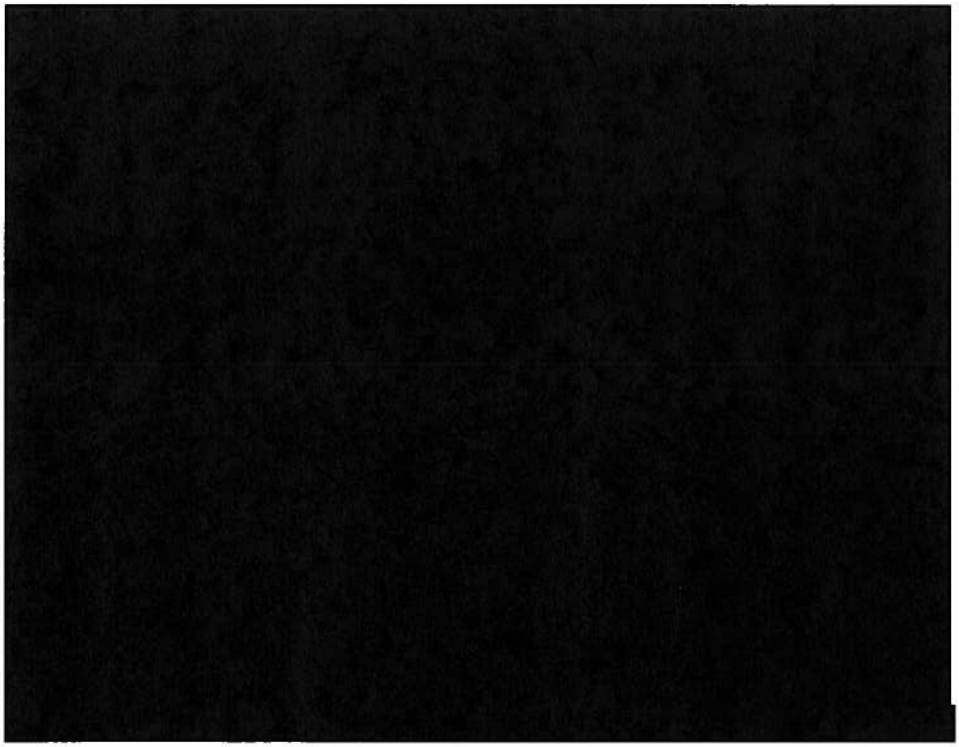
Vulnerability Remediation











[redacted]

Monthly scans provide an assessment of a system's configuration and identify the vulnerabilities that could be exploited from inside the organization. While remedying scan results may require resources and time to perform and analyze, penetration testing also requires a significant amount of resources to conduct and usually includes system scans to identify and analyze vulnerabilities for exploitation. Additionally, only a limited number of vulnerabilities may be identified and tested during penetration testing because its scope usually does not include all the components' systems. By contrast, monthly scans show systemic vulnerabilities throughout the Department and its components.

[redacted]

[redacted]

The Department's Monitoring and Oversight

To ensure that the documented IT security program is implemented throughout its components, the Department has developed various monitoring and oversight procedures including the ITSC, the POA&M process, the OCIO reviews, and the Dashboard. As detailed in the following sections, we reviewed each procedure to determine its effectiveness in monitoring the implementation of the Department's IT security program.

Information Technology Security Council

The ITSC is the central focal point of the Department's IT Security Program. The ITSC is a team, composed of the CISO from each component and led by the Department's Deputy CIO for IT security, which manages the Department's IT security priorities and compliance with government policies and regulations.

We interviewed CIOs and ISSOs from 10 of the 26 Department components for their assessment of whether the ITSC is functioning as envisioned. According to 6 of the 10 CIOs interviewed, the ITSC is not operating as a collaborative forum for decision-making. Instead, according to the CIOs, it is a venue used by the Department to inform components of decisions that were already made.

The Assistant Director of the Enterprise Solutions Team of ITSS stated that the Department established project teams as an extension of the ITSC to allow the components to participate in the decision-making process.[37] Each Department component is represented by a team member with responsibilities in a particular project team area, who presents component concerns. For example, the Computer Environment and Enclave Defense (CEED) team meets monthly to discuss IT security policy changes and pending implementation of new IT security tools. The meetings are intended to solicit feedback from the components on the issues at hand. The Assistant Director stated that the CEED monthly meetings are well-attended by the components with 25 to 30 representatives participating. The component representatives are expected to share with their CIOs the information that is discussed in the meetings. If the CIO is concerned about the decisions made in the meeting, the CIO can voice concerns to the Department's CIO. Yet, we found that despite this process, the CIOs still

[37] The project teams are: IT Security Employee Services, Computing Environment and Enclave Defense, Department Computer Emergency Readiness Team/Cyber Defense Operations, Certification and Accreditation team, Configuration Management, and IT Contingency Planning.

believe that in most cases they are not given the opportunity to provide input into decisions that could affect their funding and personnel resources.

In July 2007, the Department commissioned a contractor to perform an independent review of the Department's IT security program and provide recommendations for improvements. The report concluded that in order for the Department to reach its desired goals of anticipating and effectively monitoring changes in the information security environment and strengthening the IT security controls environment of the Department while maintaining current compliance achievements, the ITSC should use a collaborative approach, with the participation of component decision-makers who understand the mission impact of the security decisions. The report stated that the lack of accountability and authority to implement and enforce security initiatives could result in ineffective risk management and lack of assurance for the protection of critical assets.

According to the Deputy Director of ITSS, the Department is in the process of restructuring the ITSC as proposed by the independent contractor's report. However, at the time of our audit, he did not provide details on how the Department would make those changes.

Plans of Action and Milestones

Plans of Action and Milestones (POA&M) are used to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective actions on security weaknesses found in programs and systems. According to OMB guidelines, POA&Ms should list all identified weaknesses and show estimated resource needs or other challenges to resolving them, key milestones and completion dates, and the status of corrective actions.

In an August 2007 report, GAO concluded that the Department did not consistently use the POA&M process to manage the correction of its IT security actions. Specifically, the Department had not fully ensured: (1) that IT security weaknesses were addressed in a timely manner and received appropriate resources or (2) that when an IT security weakness was identified, program officials developed, implemented, and managed POA&Ms for their systems. In addition, the Department did not ensure that the POA&Ms were accurate and complete for sensitive and unclassified systems.

The Department's response to the GAO report stated that the transition from an earlier NIST control framework to that in the most recent

NIST guidance resulted in duplicate versions of the POA&Ms.[38] The response stated that CSAM does not permit easy reconciliation of these redundancies because it has no automated process to do so. As a result, the Department is challenged in accurately tracking information security weaknesses. The report concluded that without accurate tracking, the Department has little assurance that security weaknesses are being addressed appropriately.

OMB also requires agencies to prepare and submit quarterly updates to POA&Ms addressing all weaknesses identified during the annual program review and independent evaluations required by FISMA, as well as those weaknesses discovered during other reviews such as GAO audits, financial system audits, and critical infrastructure vulnerability assessments. We concluded that the Department's decision to remove the POA&M requirement for vulnerabilities identified during the scanning process eliminates a structured process for monitoring known critical vulnerability remediation, is contrary to the OMB POA&M requirement, and makes the Department's quarterly POA&M reporting to OMB incomplete and inaccurate.

The Assistant Director of the Enterprise Solutions Team of ITSS told us that the Department eliminated the requirement for POA&Ms for vulnerabilities identified through the scanning process because the vulnerability assessment control for NIST compliance does not require remediation plans for identified vulnerabilities; it only requires that the vulnerability be identified. Therefore, to be FISMA-compliant, a component does not have to show remediation plans for vulnerabilities identified through the scanning process.

In our opinion, a structured process for monitoring vulnerability remediation would improve the accuracy of the Department's assessment of the security controls environment of its systems, and we recommend that the Department's CIO establish a mechanism for monitoring remediation of all identified IT system vulnerabilities.

Office of the Chief Information Officer Reviews

As part of its monitoring and oversight of the implementation of the Department's IT security program, the ITSS conducts two reviews: (1) the review of C&A documentation, and (2) the annual OCIO review of selected quality controls, which are chosen by the IT Security Council. As an added

---

[38] Initially, NIST SP 800-26, *Security Self-Assessment Guide for Information Technology Systems* provided the information security control framework for federal agencies. It was replaced in 2006 by the information security control framework described in NIST SP 800-53.

measure designed to ensure compliance with Department policy and standards, the OCIO also reviews self-assessments conducted by the Department's components.

Certification & Accreditation Review

The OCIO and the ITSS management team conduct periodic reviews of C&A packages of component systems to verify that the package is accurate and the risks accepted by the authorizing official are acceptable. These reviews also identify how the component is addressing the vulnerabilities identified in the system. The vulnerabilities are for those identified during the C&A process and not the monthly scans. This review typically occurs just before the OIG conducts the yearly FISMA audits.

Annual OCIO Reviews

FISMA requires that the management, operational, and technical controls in each information system be assessed with a frequency depending on risk, but no less than annually. Sources of these assessments include security certification testing in support of accreditation or re-accreditation, continuous monitoring activities, and testing and evaluation as part of the ongoing system development life cycle process. The number of controls reviewed for the annual assessment is determined each fiscal year by the ITSC, who approves a minimum selection of controls for continuous monitoring or annual assessment.[39] The selected controls are reviewed throughout the year to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome to meet the security requirements for the system.

Controls not selected may also be reviewed at the discretion of the ITSS. The decision to review any of the unselected controls is based on several factors, including criticality to security; successful implementation of the control historically; the security category of the system (low, medium, or high); and the depth of the previous year's review. Additionally, some controls are reviewed more frequently, such as those dealing with vulnerability scanning, system configuration management, patch management, and incident reporting. Most commonly, the ITSS reviews C&A documentation, documentation supporting the component's successful implementation of a control, and POA&Ms to determine compliance with applicable guidelines. The ITSS documents the results of the reviews in the CSAM tool kit.

[39] See Appendix II for a list of controls selected for monitoring during FY 2007.

During the review of C&A documentation, OCIO reviewers ensure that the data in CSAM matches the data in the System Security Plan and C&A documentation, and that pertinent items are uploaded to CSAM or a reference to their location is noted. If during the review a deficiency is found, the ITSS documents the deficiency in the appropriate fields of CSAM and notifies the system owner or ISSO of the difference of opinion. The interested parties discuss the differences and, if agreement is achieved, any necessary updates to the review results are made.

The OCIO reviewer also reviews any documentation showing that a control was successfully implemented. If a control test shows "failed" in CSAM, the ITSS verifies that a POA&M was completed and reviews the resulting POA&M for adequacy and completeness of required fields. If the OCIO reviewer determines that the compensating controls identified in the POA&M do not sufficiently mitigate the risk, a waiver request must be submitted to and approved by the Department's CIO. However, if the review is being conducted at a component's site and a deficiency is identified, and the deficiency can be resolved by the appropriate party and re-evaluated by the reviewer during the duration of the control reviews, a POA&M is not required. On the other hand, if the discrepancy cannot be resolved, a POA&M is required to address the deficiency.

To ensure that previously established POA&Ms meet the requirements of the Department and OMB, OCIO reviewers review all system POA&Ms in CSAM. By reviewing the POA&M, OCIO reviewers ensure that a point of contact has been identified, cost data is captured for the POA&M, a scheduled completion date has been established, and the source of the POA&M has been recorded. The reviewer provides the party responsible for the POA&M with any data deficiencies. As previously noted, the Department is responsible for reporting the status of all POA&Ms to OMB on a quarterly basis. Therefore, once a POA&M has been reported to OMB, its scheduled completion date cannot be changed. The OCIO reviewers are responsible for ensuring that the scheduled completion date is not changed.

Upon conclusion of the review, the reviewer must provide a report to the system owner and ISSO (or higher official if desired by the component), including the:

1. results of security control evaluation, including review comments for all controls reviewed, comments regarding missing or deficient information, recommendations for improvement if needed, and positive comments where warranted; and

2. requirements for POA&Ms to be developed based on the review.

It is important to note that the POA&Ms reviewed by OCIO reviewers are those resulting from C&A activity, which does not include monthly scanning for vulnerabilities. The components are responsible for tracking the remediation of vulnerabilities identified from the monthly scans, which are not recorded in CSAM. Since the information on monthly scans is not recorded in CSAM, ITSS does not review the status of related vulnerability remediation during the OCIO annual review.

According to the IT Security Program Management Plan, the Department should conduct OCIO reviews very close to the time that the OIG conducts its annual FISMA review. Because Congress uses the results of the OIG reviews to calculate the overall FISMA score for the Department, the components believe that most attention is placed on IT security at this point.[40] The CIOs stated that the overemphasis on POA&M completion, control testing, and ensuring that each system has an updated authority to operate are all done at this time to ensure that the Department looks good to the auditors and eventually to OMB. Component CIOs contend that more time is spent on updating the paper requirements as opposed to working on real security issues.

OMB grades an agency's compliance with FISMA requirements in seven areas on a 100-point scale. The seven areas include annual testing, POA&Ms, C&A, configuration management, incident detection and response, training, and inventory. The Department received an A^+ grade for FY 2007, an A^- for FY 2006, and a D for FY 2005. As noted above, FISMA focuses primarily on ensuring that policies and procedures are in place to secure the information contained in the IT systems; it does not measure the implementation and effectiveness of these policies and procedures.

For example, to receive the maximum 20 points in the area of configuration management, an agency must: (1) have an agency-wide security configuration policy, and (2) ensure that special procedures for using emerging technologies and countering emerging threats are documented in its security policies. FISMA is not concerned with whether or not the agency's configuration policy meets the minimum configuration requirements for federal systems or if the agency's systems are configured according to the policy. These two questions correspond more with the implementation and effectiveness of the established policies and procedures.

---

[40] The House Committee on Oversight and Government Reform compiles the results of the audits and produces an annual report card. The report card grades are based on information contained in agency and OIG FISMA reports to OMB.

Some components' CIOs contend that in an effort to maintain an A- or obtain an A on the FISMA score card, the Department concentrates too much on ensuring that the policies are updated, thereby losing focus of the real IT security issues.

In our opinion, effective IT security is not limited to establishing adequate policies and procedures. Policies and procedures are necessary to establish a methodology for securing the Department's IT systems. However, the Department must move beyond establishing written policies and procedures and ensure that they are implemented and working as intended. If the Department focuses its IT security program on the requirements of FISMA, it may succeed in obtaining an A on the FISMA score card while falling short of providing adequate security for its IT systems.

Dashboard

The Department uses CSAM to monitor its IT security program and the component's progress in meeting FISMA requirements. The ITSC Program Progress Report Card (called the Dashboard) on IT security is prepared for all Department components that develop or operate IT systems. The Department uses a three-color (red, yellow, green) methodology to grade the components' compliance in areas such as risk assessment, C&A, POA&M completion, vulnerability assessments, and incident response. The graded criteria for each project area differ based on the Department's requirements for that project area.

For example, for the vulnerability assessment project area components are graded based on how well they comply with the Department's monthly scanning requirements. As previously stated, components are required to use Foundstone to scan all assets for vulnerabilities in all information systems. Specifically, components are required to:

- scan all assets every 30 days,
- scan using the Full Vulnerability Scan Template, and
- assign vulnerabilities remediation to the responsible person or group.

The Department assigns a color grade based on the following criteria.

Green: 90 percent or above of all known assets are scanned using Foundstone. The scans meet the above requirements and are completed within a 45-day period.

Yellow: 85 to 89 percent of all known assets are scanned using Foundstone. The scans meet the above requirements and are completed within a 60-day period.

Red: Scans are not completed and submitted within a 60-day period, or scans do not meet the above requirements.

Although the vulnerability assessment requirement includes assigning a responsible person or group to remediate the vulnerabilities, that requirement is not reflected in the scoring methodology. The scoring methodology only considers whether the scans were completed, not the status of actions taken to fix or mitigate the identified vulnerabilities. As a result, a component could receive a green rating for vulnerability assessment without doing anything to improve the security of its IT systems.

Our review of the February 2008 Dashboard showed that 20 components had a green rating, 4 had a yellow rating, and 2 were not applicable for vulnerability assessments. We believe that while the Dashboard rating methodology may be effective in tracking the Department's progress towards FISMA compliance, it does not provide a complete assessment of the Department's IT security environment.

According to some of the component CIOs and ISSOs we interviewed, uploading the information to CSAM that subsequently feeds into the Dashboard is just an extensive paper exercise that takes resources away from resolving real IT security issues. Several component CIOs and ISSOs believe they spend so much time ensuring that all of their paperwork is in place that it is impossible to concentrate on significant IT security issues.

Future of the Department's Vulnerability Management Program

The Department hired a contractor in July 2007 to provide recommendations on how to effectively improve the vulnerability management program. The Department also intends to include vulnerability management as part of the JSOC initiative.

Justice Security Operations Center

The purpose of the JSOC is to provide real-time monitoring of the security and network health of the Department's IT systems, proactively identify security incidents, facilitate enterprise incident response, and provide security information input to risk management decisions.

According to the Department's Chief IT Security Technologist, the Department will use the JSOC to: (1) improve its ability to respond and contain the spread of security incidents and minimize the impact to mission critical systems, (2) increase its knowledge of what is happening on the Department's networks, (3) realize cost savings through centralizing services and subject matter expertise, and (4) reduce and avoid the costs of maintaining specialized resources at each component.

The Department intends to implement the JSOC through an iterative approach of adding components and services to reach final operating capability with full implementation around the fourth quarter of FY 2009. According to the Deputy CISO, the Department spent $1.1 million in FY 2007 and has budgeted $600,000 in FY 2008 for the implementation of JSOC. However, the Department has not yet determined the total cost to fully implement the JSOC.

The JSOC would provide the following services:

Threat Management – Real-time monitoring (24 hours a day, 7 days a week) of mission critical infrastructure components to actively identify attacks and emerging threats. This service would provide a means for the Department to more proactively defend against cyber attacks and inside threats.

Vulnerability Management – Full life cycle support for the components to assist with the identification, analysis, prioritization, and remediation of security vulnerabilities. This service would provide the Department with technical expertise to analyze and prioritize vulnerability remediation based upon current and emerging threats affecting the Department.

Incident Response – Full life cycle support for security incidents Department-wide and coordination internally and externally with US-CERT. The service would provide the Department with skilled engineers to efficiently and effectively identify incident containment and mitigation strategies across the Department.

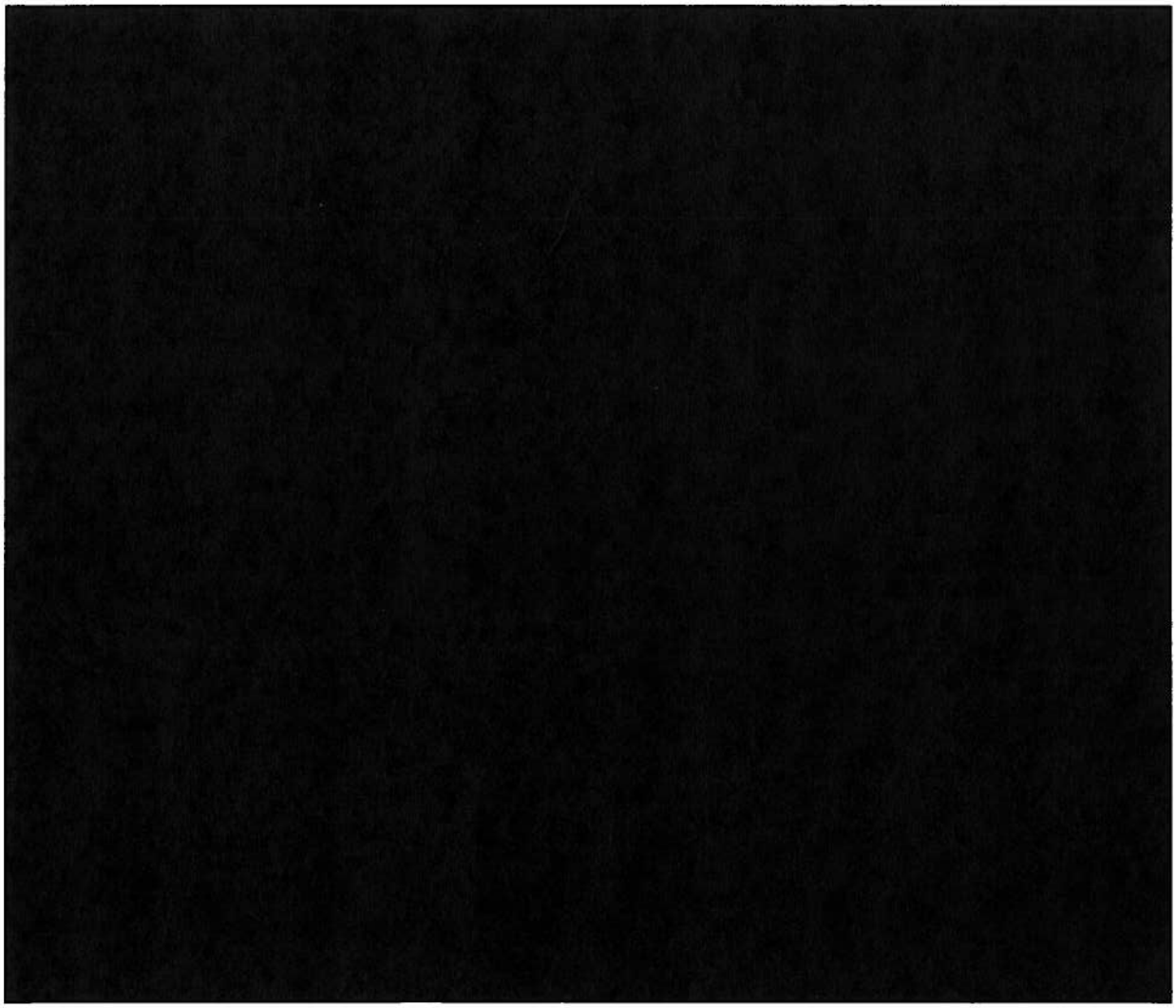
Network Monitoring – Real-time monitoring (24 hours a day, 7 days a week) of network performance and availability that identify potential impacts to network services. This service would provide the Department with the ability to proactively monitor and identify network disruptions that affect mission critical IT systems and minimize downtime.

Technical Security – The security operations center design and engineering for JSOC and managed customer devices. This service would provide the Department with managed infrastructure services to support efficient configuration of infrastructure devices.

Surge Support – Surge support would provide additional resources for short term staff augmentation, allowing component teams the ability to tap specialized resources to supplement current IT staff during peak times.

Policy and Procedures – The development of policies and procedures to ensure consistent delivery of services to components that promote quality, repeatability, and consistency.

The following is a graphic of the proposed service release schedule for JSOC.



The core technology for the success of JSOC is [redacted], a software tool that will identify systemic vulnerabilities on all Department systems that are linked to [redacted]. For example, if outdated anti-virus software is detected on a system, [redacted] has the capability to search for other systems on the network also using the outdated software. Even with the use of [redacted], the Department will continue to require monthly scans. With [redacted], system analysts will not be required to manually analyze the monthly scans. Instead, the Department will link Foundstone with [redacted] so that after components complete the monthly scans, the servers would send the scan results to [redacted], which would combine the data, thus allowing for easier data analysis.

However, successful implementation of [redacted] and JSOC depends on the components allowing the Department to monitor their networks. As of December 2007, 6 of the Department's 26 components were linked to [redacted] and were being monitored by the Department, including the BOP, OJP, ATF, and the Department's Operations Services Staff. According to the Department's Chief IT Security Technologist, the goal is to have [redacted] implemented at all the components by June 2008.[41]

In our opinion, when JSOC is fully operational, the Department's ability to enhance the security of the information contained in its IT systems will be significantly improved.

[41] [redacted]

Conclusion

The Department has documented a comprehensive IT security program, created an IT security oversight council, and implemented the CSAM tool to track and monitor FISMA compliance.

However, access controls, [redacted], and outdated patches are critical vulnerabilities within the Department. These vulnerabilities remain systemic because the Department lacks a fully effective vulnerability management program that includes a process tracking the remediation of vulnerabilities identified in the monthly system configuration scans and a methodology for applying Department-wide global fixes for known vulnerabilities. The lack of these methodologies, as well as lack of an inventory of all of the Department's networked devices, hurts the Department's ability to accurately assess the security controls environment of its IT systems and its ability to secure its IT systems and information resources.

Recommendations

We recommend that the Department:

1. Implement a structured process for monitoring and tracking the remediation of critical vulnerabilities identified during the monthly scanning process.

2. Ensure the new monitoring process includes a detailed review and analysis of all identified critical vulnerabilities.

3. Develop a system that provides real-time monitoring of the IT security environment, proactively identifies security vulnerabilities and incidents, and distributes Department-wide global fixes for known vulnerabilities.

4. Obtain an inventory of all Department-wide networked devices and update the inventory annually to reflect changes in the IT security environment.

STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS

This audit assessed the Department's major systemic IT security vulnerabilities and its progress toward mitigating the identified vulnerabilities, monitoring and overseeing IT security, and improving the overall IT security environment. The audit was conducted in accordance with *Government Auditing Standards*. As required by the standards, we reviewed management processes and records to obtain reasonable assurance about the Department's compliance with laws and regulations that could have a material effect on its operations. Compliance with laws and regulations applicable to the Department's IT systems is the responsibility of the Department's Office of Chief Information Officer management.

Our audit included examining, on a test basis, evidence about laws and regulations. The specific laws and regulations against which we conducted our tests are contained in:

- *Federal Information Security Management Act of 2002 (FISMA)*
- Office of Management and Budget Circular A-130
- *Clinger-Cohen Act of 1996*
- *E-Government Act of 2002*
- All applicable National Institute of Standards and Technology (NIST) standards and guidelines
- Federal Information Processing Standards Publication (FIPS) 199
- FIPS 200

Our audit identified no areas where the Department was non-compliant with the laws and regulations referred to above. With respect to those areas not reviewed, nothing came to our attention that caused us to believe that Department management was not in compliance with the laws and regulations cited above.

STATEMENT ON INTERNAL CONTROLS

In planning and performing our audit, we considered the Department's internal controls for determining our audit procedures. This evaluation was not made for the purpose of providing assurance on the internal control structure as a whole. However, we noted certain matters that we consider to be reportable conditions under the *Government Auditing Standards*.

Reportable conditions involve matters coming to our attention relating to significant deficiencies in the design or operation of the internal control structure that, in our judgment, could adversely affect the Department's ability to manage its IT systems. As discussed in the Findings and Recommendations section of this report, we found that the Department:

- does not have a structured process for monitoring and tracking the remediation of critical vulnerabilities identified during the monthly scanning process.

- does not perform a detailed review and analysis of all identified critical vulnerabilities.

- needs to develop a system that provides real-time monitoring of the IT security environment, proactively identifies security vulnerabilities and incidents, and distributes Department-wide global fixes for known vulnerabilities.

- needs to conduct an inventory and maintain a log of all Department-wide networked devices. The log should be updated periodically to reflect changes in the IT security environment.

Because we are not expressing an opinion on the Department's internal control structure as a whole, this statement is intended solely for the information and use of the Department in managing its IT security program. This restriction is not intended to limit the distribution of this report, which is a matter of public record.

APPENDIX I

OBJECTIVES, SCOPE, AND METHODOLOGY

Objectives

The objectives of this audit were to identify the Department's major systemic IT security vulnerabilities and assess the Department's progress towards mitigating the identified vulnerabilities, monitoring and overseeing IT security, and improving the Department's overall IT security environment.

Scope and Methodology

The audit was performed in accordance with *Government Auditing Standards*, and included tests and procedures necessary to accomplish the stated objectives. The audit generally covers the period from January 2007 through December 2007. However, we also included the results of the FY 2007 OMB FISMA report card issued in May 2008. We conducted work at the Department's Office of the Chief Information Officer and Justice Management Division in Washington, D.C.

We reviewed documents related to IT security policies and procedures, organizational structures, and prior GAO and OIG reports. We also reviewed the Department's IT Security Program Management Plan, which outlines Department, component, and system goals and responsibilities.

We interviewed officials from the Department's Office of the Chief Information Officer; Bureau of Alcohol, Tobacco, Firearms, and Explosives; Federal Bureau of Prisons; Criminal Division; Drug Enforcement Administration; Executive Office for Immigration Review; Executive Office for United States Attorneys; Executive Office for United States Trustees; Federal Bureau of Investigation; Justice Management Division; Office of Justice Programs; and United States Marshals Service.

To identify the systemic vulnerabilities within the Department, we reviewed system scan results for the entire Department. We also reviewed the Department's IT security vulnerability and incident reports for the period under review. We evaluated the procedures used to identify systemic IT security vulnerabilities in order to reveal obstacles that may impede the vulnerability identification and remediation process.

We interviewed ITSS staff, and component CIOs and ISSOs to determine whether the Department's monitoring of its IT program is adequate and whether the process contributed to the systemic nature of the vulnerabilities.

APPENDIX II

Authority to Operate (ATO) Control Standards for Certification and Accreditation

Certification, Accreditation, and Security Assessment Policies and Procedure(CA-01)	
CA-01.01-01	The security assessment, certification, and accreditation policy and procedures exist and document the purpose, scope, roles, responsibilities, compliance and review/change history. The security assessment and certification and accreditation policies and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The documents are disseminated to appropriate elements within the organization. (NIST 800-53)
CA-01.01-02	The security assessment, certification, and accreditation policies and procedures are reviewed at least annually by responsible parties within the organization and are updated, when organizational review indicates updates are required. (NIST 800-53)
Security Assessments (CA-02)	
CA-02.01-01	Assessment of security controls is conducted annually and/or when a significant change occurs, and the results are documented in the Department-approved Cyber Security Assessment and Management (CSAM) Toolkit tool(s) as specified in the current Department IT Security Program Management Plan. (NIST 800-53)
CA-02.01-51	The security controls in the information system are assessed for producing the desired outcome with respect to meeting the security requirements for the system in accordance with applicable policies and procedures. Security assessment activities are consistent with the Department security assessment procedures for breadth and depth considerations described in the Program Official and CIO Annual FISMA ATO Quality Review Procedures. (NIST 800-53)

Information System Connections (CA-03)	
CA-03.10-01	An MOU/A and ISA has been created and is up-to-date for all Department IT systems that have direct connections to two or more systems for the purpose of sharing data and other information resources. (NIST 800-53)
CA-03.02-51	Records indicate that activities for monitoring/controlling connections to information systems outside the accreditation boundary are consistent with the organization's procedures. (NIST 800-53)
CA-03.4-01	The organization assigns responsibilities and defines specific actions to ensure that external information system connections are authorized, monitored, and controlled. (NIST 800-53)
CA-03.06-01	The written agreement shall define (i) the responsibilities and controls that must be maintained for the system interconnection, including at a minimum, the management, operation and use of the interconnection, (ii) how data is shared between interconnected systems, and (iii) approval. (NIST 800-53)
CA-03.08-01	All connections to information systems outside of the accreditation boundary are authorized and approved by the appropriate organizational officials. (NIST 800-53)
CA-03.09-01	The system interconnection agreement is included in the system security plan. (NIST 800-53)
Security Certification (CA-04)	
CA-04.01-01	The certification process is integrated into and spans the System Development Life Cycle (SDLC). The certification process determines the effectiveness of each security control in the information system regarding correct implementation, intended operation, and is producing the desired outcome with respect to meeting the security requirements of the system. (NIST 800-53)
CA-04.03-01	The results of security control assessments, the specific actions taken or planned to correct deficiencies in the security controls, and actions taken or planned to eliminate known vulnerabilities in the information system are documented in the Department-approved Cyber Security Assessment and Management (CSAM) Toolkit tool(s) over time as follows: Assessment of security controls is conducted annually and/or when a significant change occurs, and the results are documented in the Department-approved CSAM Toolkit tool(s) as specified in the Department's current IT Security Program Management Plan. (NIST 800-53)

CA-04.04-01	The organization assigns responsibilities and defines specific actions to ensure that security certifications are conducted and meet their required function or purpose. Responsibility assignment is documented in the Department-approved CSAM Toolkit tool(s) as specified in the Department's current IT Security Program Management Plan. (NIST 800-53)
Plan of Action and Milestones (CA-05)	
CA-05.01-01	The organization develops and updates an action plan for the information system within the organization-defined frequency and appropriate officials know of their plan of action and milestone (POA&M) responsibilities. (NIST 800-53)
CA-05.02-01	The corrective action plan address planned actions required to correct noted deficiencies and to reduce or eliminate known vulnerabilities in the system. (NIST 800-53)
CA-05.02-03	The corrective action plan shall be created within 30 days of the completion of the assessment. (NIST 800-53)
CA-05.03-01	The action plan to correct deficiencies in the information system security controls is implemented and defines measurable milestones that demonstrate that remedial actions are effectively implemented. (NIST 800-53)
CA-05.03-02	Corrective actions are tested again in the next 6 to 12 months after they have been implemented and monitored on a continuing basis. (NIST 800-53)
CA-05.05-01	The organization assigns responsibilities and defines specific actions to ensure that a POA&M is developed, implemented, and updated for the information system. (NIST 800-53)
Security Accreditation (CA-06)	
CA-06.03-02	The system is accredited prior to operation and a senior organizational official has signed and approved the security accreditation. (NIST 800-53)
CA-06.03-03	The accreditation is updated at least every three years or when major security changes are made or when significant security breaches occur. (NIST 800-53)

CA-06.04-01	The organization assigns responsibilities and defines specific actions to ensure that security accreditations are conducted and meet their required function or purpose.
Continuous Monitoring (CA-07)	
CA-07.03-01	The assessment(s) of ATO Quality controls as defined in the Department's IT Security Program Management Plan are documented in the Department-approved Cyber Security Assessment and Management (CSAM) Toolkit tool(s) for control monitoring. (NIST 800-53)
CA-07.03-02	Changes to or deficiencies in the operation of the security controls as a result of system configuration changes or evolving threats are analyzed for impact, documented, and reported in the Department-approved CSAM Toolkit tool(s) as specified in the current Department IT Security Program Management Plan. (NIST 800-53)
CA-07.05-01	The organization assigns responsibilities and defines specific actions to ensure that security control monitoring is conducted and meets its required function or purpose. (NIST 800-53)

APPENDIX III

ACRONYMS

ATF	Bureau of Alcohol, Tobacco, Firearms & Explosives
ATO	Authority to Operate
BOP	Federal Bureau of Prisons
C&A	Certification and Accreditation
CEED	Computing Environment & Enclave Defense
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CSAM	Cyber Security Assessment and Management
Dashboard	ITSC Program Progress Report Card
Department	Department of Justice
EOUSA	Executive Office for United States Attorneys
ESOC	Enterprise Security Operations Center
FBI	Federal Bureau of Investigation
FISMA	Federal Information Security Act of 2002
FY	Fiscal Year
GAO	Government Accountability Office
ISSO	Information System Security Officer
IT	Information Technology
ITSC	Information Technology Security Council
ITSS	Information Technology Security Staff
JSOC	Justice Security Operations Center
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Department of Justice Office of the Inspector General
OMB	Office of Management and Budget
POA&M	Plans of Action and Milestones
SDLC	System Development Life Cycle
USMS	United States Marshals Service
VM Plan	Vulnerability Management Plan

APPENDIX IV

THE DEPARTMENT'S RESPONSE TO THE DRAFT REPORT

U.S. Department of Justice

Washington, D.C. 20530

November 7, 2008

MEMORANDUM FOR RAYMOND J. BEAUDET
ASSISTANT INSPECTOR GENERAL FOR AUDIT

FROM: Vance E. Hitch
Chief Information Officer

SUBJECT: Draft Audit Report - Department of Justice Efforts in Managing Information Technology Security Vulnerabilities

We have received and reviewed your Draft Audit Report as captioned above, dated October 20, 2008. Since the audit was conducted in the spring of 2007, the Department has taken a number of initiatives related to managing the security of the Department's IT systems.

One of these initiatives is the creation of an IT security governance structure to support the IT security program. It provides a collaborative approach to IT security through the IT Security Governance Council (ITSGC), which provides a forum and process for enhancing communications with the Component CIOs, for identifying high priority IT security-related topics, and for providing informed advice to the DOJ CIO. This informed advice helps to improve risk-based decisions for IT security governance and risk management, as well as to manage expectations and align the strategies of IT stakeholders across the Department.

Another initiative, the Justice Security Operations Center (JSOC) is fully operational and provides real-time monitoring of the Department's IT security environment. The JSOC provides threat and vulnerability management, as well as incident response support for the Department. We continue to strive to improve the IT security vulnerability management process at DOJ.

The report's recommendations are addressed below:

Recommendation 1: Implement a structured process for monitoring and tracking the remediation of critical vulnerabilities identified during the monthly scanning process.

JMD Response - We concur. The IT Security Staff (ITSS) has identified an exceptional framework for vulnerability management at the Office of Justice Programs. The implementation of this framework is currently being piloted at several components. Once testing of this framework is completed, ITSS will provide it for use across the Department. The framework is based on utilizing a vulnerability tracking tool to track critical vulnerabilities "cradle to grave", showing status of implementation and remediation for fix actions. There will be additional standard operating procedures (SOPs) for remediation of vulnerabilities to follow. The framework for these SOPs and the tracking tool will be provided to DOJ Components by January 31, 2009. Components can use this framework for their processes if deficiencies are identified in their vulnerability management program. In addition, a critical vulnerability tracking tool will be used for the enterprise. A version of this tool will be implemented in calendar year 2009.

Recommendation 2: Ensure the new monitoring process includes a detailed review and analysis of all identified critical vulnerabilities.

JMD Response - We concur. The new vulnerability management (VM) framework (from Recommendation 1) will include requirements for security and operations reviews of new identified critical vulnerabilities as they emerge. These reviews will involve representatives from the DOJCERT (Justice Security Operations Center), the Computing Environment and Enclave Defense (CEED) team, and operations as allowed. The vulnerabilities will be analyzed for threat to the DOJ enterprise and actions will be taken as appropriate. Additionally the framework will call for a bi-monthly vulnerability management meeting to discuss current vulnerabilities affecting the enterprise. Guidelines for these meetings will be outlined in the enterprise VM framework set for release by January 31, 2009.

Recommendation 3: Develop a system that provides real-time monitoring of the IT security environment, proactively identifies security vulnerabilities and incidents, and distributes Department-wide global fixes for known vulnerabilities.

JMD Response - We concur and consider this finding closed. Real time monitoring of the IT security environment is accomplished by the Justice Security Operations Center (JSOC), which was brought online in October 2007. The JSOC uses Security Information and Event Management software with multiple real-time feeds from vulnerability management software,

antivirus software, etc. This enables ITSS to proactively identify vulnerabilities that affect the enterprise. In addition, global fixes for known vulnerabilities are applied by patch management solution systems.

Recommendation 4: Obtain an inventory of all Department-wide networked devices and update the inventory annually to reflect changes in the IT security environment.

JMD Response - We concur. The department will gather an initial inventory of all DOJ assets on the enterprise by January 31, 2009, utilizing existing network discovery software applications. This information will be used to create secure baselines based on best practices and guidelines from NIST, DISA, etc.

Thank you for the opportunity to comment on the draft report.

APPENDIX V

OFFICE OF THE INSPECTOR GENERAL ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE THE REPORT

The OIG provided a draft of this audit report to the Department of Justice, Office of the Chief Information Officer (Department) on October 20, 2008, for its review and comment. The Department's November 10, 2008, response is included as Appendix IV of this final report. The Department concurred with the four recommendations in the audit report and based on the Department's response, the OIG considers the report resolved. Our analysis of the Department's response to the four recommendations is provided below. The status of each recommendation and the actions necessary to close them follows:

Response to Recommendations

1. **Resolved.** The Department agreed with this recommendation. In its response, the Department stated that the IT Security Staff is piloting a vulnerability management framework at several components. The framework is based on a vulnerability tracking tool, which is capable of tracking the status of critical vulnerabilities from "cradle to grave." The Department also stated that additional standard operating procedures for remediation of vulnerabilities and an enterprise critical vulnerability tracking tool will be implemented. This recommendation can be closed when we receive documentation showing the Department has implemented a structured process for monitoring and tracking the remediation of critical vulnerabilities identified during the monthly scanning process.

2. **Resolved.** This recommendation is resolved based on the Department's agreement with the recommendation. The Department's response stated that the vulnerability management framework, as discussed in response to recommendation 1, will include requirements for security and operations reviews of newly identified critical vulnerabilities as they emerge. In addition, the Department stated that the vulnerabilities will be analyzed for threats to the DOJ enterprise and actions will be taken as appropriate. This recommendation can be closed when we receive documentation showing that the Department's structured process for

monitoring and tracking the remediation of critical vulnerabilities identified during the monthly scanning process includes a detailed review and analysis of all identified critical vulnerabilities.

3. **Resolved.** This recommendation is resolved based on the Department's agreement with the recommendation. The Department's response stated that real-time monitoring of the IT security environment is accomplished by the Justice Security Operations Center (JSOC), which was brought online in October 2007. JSOC uses Security Information and Event Management software with multiple real-time feeds that enables ITSS to proactively identify vulnerabilities. In addition, the Department's response states that global fixes for known vulnerabilities are applied by patch management solution systems. We were aware of the implementation of JSOC in December 2007 at which time 6 of the 26 Department's components were linked to JSOC. As of October 2008, [redacted] of the 26 components were linked to JSOC. In our opinion, the success of JSOC depends on the participation of all components in this initiative. This recommendation can be closed when the Department demonstrates that JSOC actually provides real-time monitoring of the IT security environment and proactively identifies security vulnerabilities and that patch management solution systems distributes Department-wide global fixes for known vulnerabilities.

4. **Resolved.** In response to this recommendation, the Department agreed to obtain an inventory of all Department-wide networked devices and update the inventory annually to reflect changes in the IT security environment. The Department said that it will gather an initial inventory of all DOJ assets on the enterprise by January 31, 2009, using existing network discovery software applications. This recommendation can be closed when we receive documentation demonstrating that an inventory of all Department-wide networked devices has been completed, and that the Department has adopted a policy of updating the inventory annually to reflect changes in the IT security environment.