



*Improvements Are Needed to the Information  
Security Program Governance Process*

**March 11, 2008**

**Reference Number: 2008-20-076**

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.



TREASURY INSPECTOR GENERAL  
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY  
WASHINGTON, D.C. 20220

March 11, 2008

**MEMORANDUM FOR CHIEF INFORMATION OFFICER**

**FROM:** *Michael R. Phillips*  
Michael R. Phillips  
Deputy Inspector General for Audit

**SUBJECT:** Final Audit Report – Improvements Are Needed to the Information Security Program Governance Process (Audit # 200620026)

This report presents the results of our review to determine whether the Internal Revenue Service (IRS) monitored compliance with security policies and procedures and developed sufficient information security guidance. This review was included in the Treasury Inspector General for Tax Administration Fiscal Year 2008 Annual Audit Plan and was part of the Information Systems Programs unit's statutory requirements to annually review the adequacy and security of IRS technology.

*Impact on the Taxpayer*

The IRS is responsible for developing an effective information security governance process that complies with Federal Government standards. The IRS could make improvements in carrying out two key aspects of this process: (1) monitoring compliance with security policies and procedures and (2) issuing security guidance for all employees to follow. Until improvements are made, security weaknesses are more likely to occur, and the IRS cannot provide assurance that systems containing sensitive taxpayer data are adequately protected from security breaches.



## *Improvements Are Needed to the Information Security Program Governance Process*

### Synopsis

The National Institute for Standards and Technology (NIST)<sup>1</sup> identifies techniques that agencies can use to monitor the status of their security programs. The IRS needs to improve its use of these techniques. For example:

- System owners are required to ensure that corrective actions are taken to resolve security weaknesses. These actions are closed with no assurance provided to IRS executives that the actions were effective.
- All devices connected to the IRS network are to be scanned quarterly for configuration compliance. Not all devices are included in the scans, and weaknesses were not documented.
- The IRS is required to semiannually analyze incidents reported, identify common weaknesses, and follow up to ensure that the weaknesses are corrected. The IRS did not always identify the causes of the 1,172 incidents reported in a 1-year period and did not always follow up to ensure that the weaknesses were corrected.
- Security controls should be tested at least annually to ensure that they are accomplishing their intended purposes. During another audit, we found 15 (75 percent) of 20 systems did not meet basic annual testing requirements.<sup>2</sup>
- Analysis of metrics should be a part of the IRS' monitoring efforts. The IRS is making progress in this area, but its metrics do not yet meet Federal Government requirements.

While the Cybersecurity organization is primarily responsible for monitoring compliance with security guidance, the Modernization and Information Technology Services organization and each of the business functions are responsible for implementing the guidance. In a bureau as large and diverse as the IRS, it is difficult for one office to enforce implementation across organizational lines. Thus, the IRS has taken insufficient actions to monitor and enforce compliance, resulting in weaknesses that put the security and privacy of taxpayer information at risk.

The NIST also provides key elements that agencies should include in their security guidance. The Cybersecurity organization developed guidance that meets standards for 9 of the 12 key elements (security areas). However, guidance for the remaining three elements (system development life cycle, capital planning, and security services and products acquisition) did not

---

<sup>1</sup> The NIST, under the Department of Commerce, is responsible for developing standards and guidelines for providing adequate information security for all Federal Government agency operations and assets.

<sup>2</sup> *Treasury Inspector General for Tax Administration - Federal Information Security Management Act Report for Fiscal Year 2007* (Reference Number 2007-20-186, dated September 4, 2007).



## *Improvements Are Needed to the Information Security Program Governance Process*

---

include all necessary considerations to meet NIST requirements and made references to obsolete standards and controls.

For any guidance to be effective, it must be communicated to those who need it. The Cybersecurity organization needs to make it easier for users to locate security policy guidance on its web site, which is the primary source for communicating security requirements. Confusion caused by difficulty in locating guidance increases the likelihood that employees could unknowingly create weaknesses that result in security breaches.

### *Recommendations*

We recommended the Chief Information Officer, through the Security Services and Privacy Executive Steering Committee, require system owners to regularly report to the Committee on progress in addressing Plans of Action and Milestones items; require the Cybersecurity organization to improve the verification of compliance with standard configurations; analyze the incidents reported to the Computer Security Incident Response Center to identify common or systemic underlying weaknesses that contributed to these incidents and track corrective actions in the appropriate Plan of Action and Milestones; ensure that system owners prepare continuous monitoring plans that implement annual testing of system controls compliant with NIST guidance; and develop quantifiable security metrics based on IRS information security goals and objectives and require that the Cybersecurity organization analyze anomalies for root causes and report its results regularly to the Committee.

To improve security guidance, we recommended the Associate Chief Information Officer, Cybersecurity, coordinate with other IRS executives, as appropriate, to include complete NIST-compliant security guidance for the three areas that need to be updated; improve the Cybersecurity organization Intranet web site by maintaining all security procedures in one location and providing direct links to other Federal Government guidance as necessary; and develop a system to notify employees and contractors of changes to security guidance.

### *Response*

IRS management agreed with our recommendations. The Associate Chief Information Officer, Cybersecurity, will use a process for monitoring progress on Plans of Action and Milestones, conduct scans every 6 weeks to identify noncompliance with security configuration standards, prepare quarterly trend reports of security incidents that identify common or systemic weaknesses, develop a process for validating system owners' compliance with the IRS' continuous monitoring procedures, and develop and analyze quantifiable security metrics. The Security Services and Privacy Executive Steering Committee will take an active role in overseeing these activities and use the results to improve security in the IRS. In addition, the Associate Chief Information Officer, Cybersecurity, will develop guidance for the three areas



## *Improvements Are Needed to the Information Security Program Governance Process*

---

that need to be updated, improve the Cybersecurity organization Intranet web site to facilitate easy access to security guidance, and develop a system to notify employees and contractors of changes in guidance. Management's complete response to the draft report is included as Appendix IV.

Copies of this report are also being sent to the IRS managers affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions or Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs), at (202) 622-8510.



---

*Improvements Are Needed to the Information Security Program  
Governance Process*

---

*Table of Contents*

**Background** .....Page 1

**Results of Review** .....Page 3

    Improvements Are Needed to Monitor Compliance With Security  
    Policies and Procedures .....Page 3

Recommendation 1:.....Page 8

Recommendations 2 through 4:.....Page 9

Recommendation 5: .....Page 10

    Information Security Guidance Is Adequate, but Procedures Remain  
    Fragmented and Difficult to Locate .....Page 10

Recommendations 6 through 8:.....Page 12

**Appendices**

    Appendix I – Detailed Objective, Scope, and Methodology .....Page 14

    Appendix II – Major Contributors to This Report .....Page 15

    Appendix III – Report Distribution List .....Page 16

    Appendix IV – Management’s Response to the Draft Report .....Page 17



*Improvements Are Needed to the Information Security Program  
Governance Process*

---

*Abbreviations*

FISMA	Federal Information Security Management Act
IRS	Internal Revenue Service
NIST	National Institute for Standards and Technology
POA&M	Plan of Action and Milestones



---

## *Improvements Are Needed to the Information Security Program Governance Process*

---

### *Background*

The Internal Revenue Service (IRS) relies extensively on computer systems to support its financial and mission-related operations. In Fiscal Year 2006, the IRS collected \$2.5 trillion in tax payments, processed millions of tax and information returns, and paid about \$277 billion in refunds to taxpayers. It also collects and maintains a significant amount of personal and financial information on each American taxpayer. The confidentiality of this sensitive information must be protected so that taxpayers are not exposed to loss of privacy and/or to financial loss and damages resulting from identity theft and other financial crimes.

Congress and the Office of Management and Budget instituted a number of laws, regulations, and directives that govern the establishment and implementation of Federal Government information security practices. These laws, regulations, and directives establish Federal Government and agency-level responsibilities for information security, define key information security roles and responsibilities, identify minimum information security controls, specify compliance-reporting rules and procedures, and provide other essential requirements and guidance. They also provide an infrastructure for developing and promulgating detailed standards and implementation guidance to Federal Government agencies through the National Institute for Standards and Technology (NIST).<sup>1</sup>

The NIST developed the *Information Security Handbook* (Special Publication 800-100) based on laws and regulations relevant to information security, including the Clinger-Cohen Act of 1996,<sup>2</sup> the Federal Information Security Management Act (FISMA),<sup>3</sup> and Office of Management and Budget Circular A-130, *Management of Federal Information Resources*.<sup>4</sup> The purpose of the NIST *Handbook* is to assist managers in establishing and implementing an information security governance program, in compliance with regulations, that supports the agency mission in a

---

<sup>1</sup> The NIST, under the Department of Commerce, is responsible for developing standards and guidelines for providing adequate information security for all Federal Government agency operations and assets.

<sup>2</sup> (Federal Acquisition Reform Act of 1996) (Information Technology Management Reform Act of 1996), Pub. L. No. 104-106, 110 Stat. 642 (codified in scattered sections of 5 U.S.C., 5 U.S.C. app., 10 U.S.C., 15 U.S.C., 16 U.S.C., 18 U.S.C., 22 U.S.C., 28 U.S.C., 29 U.S.C., 31 U.S.C., 38 U.S.C., 40 U.S.C., 41 U.S.C., 42 U.S.C., 44 U.S.C., 49 U.S.C., 50 U.S.C.). The Act requires agencies to use a disciplined capital planning and investment control process to acquire, use, maintain, and dispose of information technology resources and to establish a position of Chief Information Officer.

<sup>3</sup> Pub. L. No. 107-347, Title III, 116 Stat. 2946 (2002). The FISMA is the primary legislation governing Federal Government information security programs, building upon earlier legislation through added emphasis on the management dimension of information security.

<sup>4</sup> Circular A-130 establishes a minimum set of controls to be included in Federal Government automated information security programs, assigns Federal Government agency responsibilities for the security of automated information, and links agency automated information security programs and agency management control systems.





## *Improvements Are Needed to the Information Security Program Governance Process*

---

cost-effective manner. The NIST guidance summarizes security responsibilities for key executives, including the Agency Head, Chief Information Officer, and Senior Agency Information Security Officer.

From October 2003 until July 2007, the IRS Senior Agency Information Security Officer and the Chief Information Officer led two separate organizations. The IRS Mission Assurance and Security Services organization was formed in October 2003 to bring together previously separate security functions and enable a consistent, unified approach to information security. The Chief, Mission Assurance and Security Services, carried out the responsibilities of the Senior Agency Information Security Officer. Within the Mission Assurance and Security Services organization, the Information Technology Security Program Office was responsible for interpreting Office of Management and Budget, NIST, FISMA, and Department of the Treasury requirements and for establishing security guidance, tracking compliance, monitoring program implementation, and providing day-to-day support.

On July 8, 2007, the IRS dissolved the Mission Assurance and Security Services organization and transferred responsibility for computer security to the Modernization and Information Technology Services organization. The Associate Chief Information Officer, Cybersecurity, now performs the role of Senior Agency Information Security Officer and reports to the Chief Information Officer. The Associate Chief Information Officer, Cybersecurity, also leads the Security Services and Privacy Executive Steering Committee, which is comprised of IRS executives from all business and functional units and the Modernization and Information Technology Services organization. This Committee serves as the primary governance body for all matters relating to security and privacy issues in the IRS. Hereafter, we will refer to the Cybersecurity organization in this report because the Mission Assurance and Security Services organization was dissolved during our review.

This review was performed at the office of the Associate Chief Information Officer, Cybersecurity, in New Carrollton, Maryland, during the period September 2006 through December 2007. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.



---

*Improvements Are Needed to the Information Security Program  
Governance Process*

---

## *Results of Review*

### ***Improvements Are Needed to Monitor Compliance With Security Policies and Procedures***

An information security governance program requires constant review to be effective. According to the NIST, agencies should periodically test and evaluate the effectiveness of information security controls, procedures, and practices. The information technology security staff should monitor the status of security programs to ensure that (1) ongoing security activities are providing appropriate support to the agency mission, (2) procedures and controls are current and aligned with evolving technologies, (3) and controls are accomplishing their intended purpose.

To facilitate ongoing monitoring, the NIST provides examples of methods that agencies such as the IRS can use to monitor the status of their security programs. These include:

- Plan of Action and Milestones (POA&M).
- Configuration management.
- Incident and event statistics.
- Continuous assessment.
- Measurement and metrics.

The office of the Associate Chief Information Officer, Cybersecurity, includes aspects of all these methods as part of its monitoring plan. However, more work needs to be done in each of these areas to ensure that the IRS information security governance program is being effectively implemented. We identified the following concerns with the IRS' current methods for monitoring compliance with security guidance.

#### ***Verification is not obtained to ensure that weaknesses identified in POA&Ms are resolved***

The Office of Management and Budget requires weaknesses identified during security assessments to be documented in POA&Ms, which are to be reviewed quarterly. Progress to correct deficiencies and eliminate known vulnerabilities should be tracked until resolution. The POA&Ms can assist in identifying performance gaps, evaluating an agency's security performance and efficiency, and conducting oversight.

Quarterly, the IRS reports to the Department of the Treasury on its total number of POA&M weaknesses and the number of weaknesses for which corrective actions have been taken, are ongoing, or have been delayed, as reported by system owners. However, when system owners



---

## *Improvements Are Needed to the Information Security Program Governance Process*

---

report that they have corrected weaknesses, the Cybersecurity organization does not receive supporting documentation to verify whether the corrective actions have in fact been taken and whether the actions resolved the weaknesses.

In March 2007, the Department of the Treasury issued guidance requiring that recently closed actions on weaknesses be incorporated into the annual testing plans for the related systems. This action should help verify that POA&M items are properly closed.

Without verification that weaknesses have been corrected, the Cybersecurity organization cannot monitor progress toward improving the security of IRS systems and the information they process and store. Government Accountability Office and Treasury Inspector General for Tax Administration reports continue to describe persistent security weaknesses that place the IRS at risk of disruption, fraud, and/or inappropriate disclosure of sensitive information. In March 2007, the Government Accountability Office reported that the IRS had made only limited progress toward correcting or mitigating previously reported information security weaknesses.<sup>5</sup> Followup audits have found that, in some cases, corrective actions were taken but did not effectively resolve the weaknesses. In at least one instance in Fiscal Year 2007, we found a previously reported condition had been closed off the IRS program-level POA&M, although corrective actions had not been taken.<sup>6</sup>

### **Verification of configuration compliance needs to be improved**

The IRS has standard configurations for most operating systems and devices connected to its network. It relies on system administrators located throughout the country to maintain those configurations. Configuration monitoring is an essential component for identifying potential security-related problems in information systems. To identify noncompliance with configuration standards, in October 2005 the Cybersecurity organization implemented a requirement for all computing devices connected to the IRS network to be scanned quarterly for configuration compliance.

The IRS primarily uses two types of scans: vulnerability scans and compliance checkers. Vulnerability scans are run from a remote scanning system and check systems for a series of vulnerabilities based on the SANS Top 20 Vulnerability List.<sup>7</sup> The compliance checker tool can be run locally or remotely on target systems and checks the systems for operating system configurations. Both types of scans are run quarterly.

---

<sup>5</sup> *Information Security: Further Efforts Needed to Address Significant Weaknesses at the Internal Revenue Service* (GAO-07-364, dated March 2007).

<sup>6</sup> *Insufficient Attention Has Been Given to Ensure States Protect Taxpayer Information* (Reference Number 2007-20-134, dated August 31, 2007).

<sup>7</sup> The SANS (SysAdmin, Audit, Network, Security) Institute, established in 1989, develops and maintains the largest collection of research documents about various aspects of information security.



---

## *Improvements Are Needed to the Information Security Program Governance Process*

---

The decision to perform scans quarterly was a step in the right direction, although some large organizations run these scans daily. The Modernization and Information Technology Services organization has field office staffs that execute the compliance checker tools on the various IRS operating systems. The results of the compliance checker tools are documented in action plans. However, weaknesses identified during quarterly vulnerability scans were not documented in system POA&Ms to ensure proper tracking and resolution. Security configuration weaknesses that are not properly tracked may leave the IRS at increased risk of security breaches.

Also, not all types of operating systems and network devices are included in the quarterly scans. For example, the IRS only recently acquired a tool to scan databases for compliance with standard configurations. In addition, running the scans quarterly is not frequent enough to ensure that weaknesses are discovered quickly. Furthermore, scans are regularly scheduled and predictable, thereby detracting from the reliability of the results for making an accurate assessment of the compliance with standard configurations.

In our Fiscal Year 2007 FISMA report, we reported that the IRS has security configuration guidance but needs to do more to ensure information systems apply common security configurations.<sup>8</sup> In another recent review, we evaluated database configuration controls and found security configurations were not adequately implemented.<sup>9</sup> Database security configurations were poorly communicated, security roles and responsibilities were not assigned or carried out, and tests to detect noncompliance with standard configurations were inadequate.

### **Incident and event statistics were not used to identify potential security weaknesses**

Incident statistics are valuable in determining the effectiveness of security guidance. They can identify performance trends and enable security program managers to identify the need to change controls and procedures. Incident statistics should be monitored for trends and correlated with other data sources, including network monitoring, POA&Ms, configuration management, training and awareness, and other available resources.

The Department of the Treasury requires its bureaus to semiannually analyze the incidents reported to their Computer Security Incident Response Centers, identify common underlying weaknesses that contributed to these incidents, and incorporate them into POA&Ms. Since 2006, these analyses have been due to the Department of the Treasury on May 1 and November 1 of each year.

The IRS had not completed this analysis prior to our visit in March 2007. Following our visit, the Computer Security Incident Response Center prepared for submission to the Department of

---

<sup>8</sup> *Treasury Inspector General for Tax Administration - Federal Information Security Management Act Report for Fiscal Year 2007* (Reference Number 2007-20-186, dated September 4, 2007).

<sup>9</sup> *Standard Database Security Configurations Are Adequate, Although Much Work Is Needed to Ensure Proper Implementation* (Reference Number 2007-20-129, dated August 22, 2007).



---

## *Improvements Are Needed to the Information Security Program Governance Process*

---

the Treasury a response that indicated it had reviewed 1,172 recorded Incident Reports for the period May 1, 2005, to April 12, 2006. Of those incidents, 584 (50 percent) could be attributed to noncompliance with 3 security controls:

- Incidents related to malicious code protection - 333 (29 percent).
- Incidents related to user-installed software - 133 (11 percent).
- Incidents related to spam and spyware protection - 118 (10 percent).

For each affected computer, the Computer Security Incident Response Center prepared requests to have the malicious code, unauthorized software, or spyware removed or to have the system restored. However, it determined that none of the findings warranted inclusion in a POA&M.

For the second quarter of Fiscal Year 2007, the Computer Security Incident Response Center reported that malicious code accounted for 46 percent of all incidents, with several systems being affected daily. Although malicious code and other violations were detected, the IRS did not always use this information to determine the underlying weaknesses that contributed to their existence or prepare corrective action plans for improving controls. Without proper analysis of incident statistics, the IRS cannot adequately monitor trends that may identify common underlying weaknesses or security controls that need improvement, thus increasing the risk of security breaches.

### **Federal Government requirements for continuous monitoring of system security controls have yet to be implemented**

The *Guide for the Security Certification and Accreditation of Federal Information Systems* (NIST Special Publication 800-37) requires Federal Government agencies to certify and accredit information systems every 3 years or when significant changes are made to a system. To certify a system, agencies must test the security controls to ensure that they are working effectively. A critical part of this process is the continuous monitoring of the security controls in the intervening years.

The *Recommended Security Controls for Federal Information Systems* (NIST Special Publication 800-53) requires a risk-based selection of controls to be tested annually to inform system owners about the status of security controls and identify controls that may not be operating as intended. Those security controls that are volatile or critical to protecting the system are to be assessed at least annually. All other controls are to be assessed at least once during the system's 3-year accreditation cycle. The *Guide for Assessing the Security Controls in Federal Information Systems* (NIST Special Publication 800-53a) should be used in assessing the effectiveness of the controls.

The Cybersecurity organization placed a workbook developed by the Department of the Treasury on its FISMA webpage to assist system owners in selecting and documenting their annual testing of NIST controls. The workbook provides descriptions of controls and selection criteria. However, in our Fiscal Year 2007 FISMA report, we reported that the IRS had not made



---

## *Improvements Are Needed to the Information Security Program Governance Process*

---

sufficient progress in properly implementing annual testing of security controls as part of its continuous monitoring efforts. Of the 20 information systems reviewed, only 5 (25 percent) met basic annual testing requirements. Each of the five systems was certified in Fiscal Year 2007 and underwent a thorough system test and evaluation as part of the certification process. System owners for the remaining 15 systems did not select controls to be tested using a risk-based approach, and the scopes of the tests were not sufficient to determine whether controls were working effectively.

We attribute the noncontinuous monitoring in the IRS to a lack of oversight to ensure that the system owners are held accountable for implementing the process. In addition, the Cybersecurity organization has not provided adequate direction to system owners on how to implement the process. Without proper implementation and testing of system controls, system owners cannot monitor the current status of their information systems or identify weaknesses that need to be resolved.

### **Measures and metrics are not used to monitor the effectiveness of the security program or investments**

Metrics are tools designed to improve performance and accountability through the collection, analysis, and reporting of relevant performance-related data. For information security, the metrics should provide a means to analyze the adequacy of security activities and identify possible improvement actions.

The *Security Metrics Guide for Information Technology Systems* (NIST Special Publication 800-55) provides guidance on how, by using metrics, an organization could identify the adequacy of existing security controls, controls, and procedures. It provides an approach to help management decide where to invest in security protection resources and how to identify and evaluate nonproductive controls.

Federal laws also require agencies to establish performance measures for information technology investments and to annually report performance information in business cases to the Office of Management and Budget to justify continued funding. The Office of Management and Budget reviews performance data to verify that only sound and cost-effective investments remain in the IRS information technology portfolio.

The IRS primarily uses the annual FISMA program as a tool for evaluating the effectiveness of its information security program. The FISMA requires Federal Government agencies to:

- Plan for security.
- Ensure that appropriate officials are assigned security responsibilities.
- Periodically review the security controls in their information systems.
- Certify and accredit a system prior to its starting operations and periodically after the system is deployed.



---

## *Improvements Are Needed to the Information Security Program Governance Process*

---

Although the FISMA provides various security metrics, it does not fulfill all performance measurement requirements established by NIST Special Publication 800-55. In addition, the IRS business case for justifying its \$77 million budget request for Fiscal Year 2008 did not provide planned or actual performance metrics for determining program effectiveness.

The Cybersecurity organization indicated it was waiting for the Department of the Treasury to provide guidance on developing additional performance measures. We acknowledge that metrics are generally helpful only to identify problems. For example, metrics may be developed to identify the number of security incidents, the number of weaknesses on POA&Ms that were not corrected on time, or the number of security settings that do not comply with configuration standards. Additional analysis will have to be done to identify the root causes of anomalies so the appropriate corrective actions can be identified.

While the Cybersecurity organization is primarily responsible for monitoring compliance with information security procedures and NIST guidance, the Modernization and Information Technology Services organization and each of the business functions are responsible for implementing the security guidance. In a bureau as large and diverse as the IRS, it is difficult for one office, such as the Cybersecurity organization, to enforce the implementation of its guidance across organizational lines. Thus, the IRS has taken insufficient actions to monitor and enforce compliance, resulting in weaknesses that put the security and privacy of taxpayer information at risk.

To assist and support the Cybersecurity organization, the Security Services and Privacy Executive Steering Committee should take a more active role in monitoring and enforcing compliance with information security guidance. This Committee consists of executives from the business and functional organizations who can provide different perspectives and furnish the authority needed to enforce security guidance. The Committee has already demonstrated success in implementing encryption on nearly all IRS laptop computers. We consider this action to be a significant accomplishment, particularly because it required the cooperation of all IRS business units. By assigning to this Committee accountability for regularly following up on the methods suggested by the NIST in monitoring security, the IRS could gain a clearer picture of its security posture at any given time and ultimately be in a better position to make informed decisions on implementing and enforcing the proper security standards and controls.

### ***Recommendations***

The Chief Information Officer, through the Security Services and Privacy Executive Steering Committee, should:

**Recommendation 1:** Require system owners to regularly report to the Committee on progress in addressing POA&M items. On a sample basis, the Committee should require system owners to provide documentation to demonstrate that corrective actions were adequate to resolve weaknesses.



---

*Improvements Are Needed to the Information Security Program Governance Process*

---

**Management's Response:** IRS management agreed with the recommendation. The Cybersecurity organization has developed a FISMA Dashboard to provide the current status of each FISMA activity, including progress on POA&Ms, at every Security Services and Privacy Executive Steering Committee meeting. The Cybersecurity organization will give additional focus to POA&Ms by adding an agenda item to the meeting for business units to report the progress on their open POA&M items.

**Recommendation 2:** Require the Cybersecurity organization to improve the verification of compliance with standard configurations by:

- Executing compliance checker tools and vulnerability scans more frequently than quarterly. Results should be provided to the Chief Information Officer and the Security Services and Privacy Executive Steering Committee.
- Extending scanning to evaluate database security.
- Including the results of scans in POA&Ms until issues are resolved.

**Management's Response:** IRS management agreed with the recommendation. The Cybersecurity organization will conduct scans once every 6 weeks to identify noncompliance with IRS standards for security configuration compliance and vulnerability management. In addition, it will extend scanning to evaluate database security, report scan results to both the Chief Information Officer and the Security Services and Privacy Executive Steering Committee, and track results in POA&Ms until issues are resolved.

**Recommendation 3:** Analyze the incidents reported to the Computer Security Incident Response Center to identify common or systemic underlying weaknesses that contributed to these incidents and track corrective actions in the appropriate POA&M.

**Management's Response:** IRS management agreed with the recommendation. The Computer Security Incident Response Center, based on reported incidents, will prepare quarterly trend reports that identify common or systemic underlying weaknesses that contribute to these incidents, incorporate and track these weaknesses in the appropriate POA&Ms until resolved, and provide this information to the Security Services and Privacy Executive Steering Committee.

**Recommendation 4:** Ensure that system owners prepare continuous monitoring plans that implement annual testing of system controls compliant with NIST Special Publications 800-53 and 800-53A. The testing should include closed POA&M items and other volatile controls. On a sample basis, the Committee should ensure that adequate documentation is maintained to support the test results and closure of POA&M items.

**Management's Response:** IRS management agreed with the recommendation. The IRS enterprise continuous monitoring approach requires that system owners prepare Continuous Monitoring Plans in compliance with NIST Special Publications 800-53 and





---

## *Improvements Are Needed to the Information Security Program Governance Process*

---

800-53A. This approach requires that testing include closed POA&M items and other volatile controls. The business owner will include the closed POA&M items in its annual testing. The business owner is responsible for planning and performing testing, documenting the results, and collecting and posting the evidence to the Department of the Treasury for tracking and reporting purposes.

The Cybersecurity organization will develop a process to validate that the system owners are following the enterprise continuous monitoring approach. This approach includes sampling and validating closed POA&M items by evaluating the test results and presenting the results to the Security Services and Privacy Executive Steering Committee.

**Recommendation 5:** Develop quantifiable security metrics based on IRS information security goals and objectives. The Cybersecurity organization should analyze anomalies for root causes and report its results regularly to the Committee.

**Management's Response:** IRS management agreed with the recommendation. The Cybersecurity organization will develop a process and collect quantifiable security metrics based on IRS security goals and objectives. It will analyze these metrics for the root causes of anomalies and report the results of the analyses to the Security Services and Privacy Executive Steering Committee.

### ***Information Security Guidance Is Adequate, but Procedures Remain Fragmented and Difficult to Locate***

Developing and documenting adequate security guidance is crucial for effective governance because it is the primary means by which management communicates its views and requirements. NIST Special Publication 800-100 covers 12 key aspects of information security that information security managers are expected to implement and oversee in their respective organizations. These 12 security areas were identified by the NIST as key elements in an information security governance program:

1. System development life cycle.
2. Awareness and training.
3. Capital planning.
4. Interconnecting systems.
5. Performance measures.
6. Security planning.
7. Information technology contingency planning.
8. Risk management.
9. Certification, accreditation, and security assessments.
10. Security services and products acquisition.
11. Incident response.
12. Configuration management.



---

## *Improvements Are Needed to the Information Security Program Governance Process*

---

We compared the NIST security standards for each of the 12 security areas to the information security guidance developed by the Cybersecurity organization. In general, the Cybersecurity organization has made significant progress in developing effective information security guidance that meets NIST standards for 9 of the 12 security areas.

The Cybersecurity organization is responsible for developing the security guidance for the 12 security areas. In some instances, it must work with other organizations to provide security guidance. For example, coordination is needed with other Modernization and Information Technology Services organizations to develop guidance for system development life cycle and capital planning. Coordination with the Agency-Wide Shared Services organization is required to develop guidance for acquisitions.

However, certain sections of the security procedures and controls set by these organizations were not current or complete. In particular, the Modernization and Information Technology Services and Agency-Wide Shared Services organizations' guidance did not include all necessary security considerations to meet NIST standards and, sometimes, made references to obsolete security standards and controls. Additionally, this guidance was not maintained with the information security guidance developed by the Cybersecurity organization. Instead, it was maintained separately within other Internal Revenue Manual sections.<sup>10</sup>

To be effective, guidance must be communicated to those who need it. We found it difficult to locate security policies and procedures. During two other reviews, we found instances in which employees were unaware of updated security guidance, how to locate it, and/or where to locate it. In a recent audit of IRS database security configurations, we identified cases in which IRS employees with key security responsibilities for database security configurations did not know of current IRS standards for these configurations.<sup>11</sup> We reviewed the controls and found the lack of awareness contributed to databases failing 30 percent of the over 800 security controls tested.

In another review of access controls over system administrator user accounts, we determined system administrators interviewed in April 2007 were unaware of the information security guidance to change passwords more frequently.<sup>12</sup> The Cybersecurity organization had established this guidance in December 2005. IRS employees possessing critical computer system responsibilities expressed dissatisfaction with or lack of knowledge about where to locate current security guidance.

The Cybersecurity organization's web site does not include a direct link to security guidance. Users must access different links to locate the webpage that contains security guidance. In

---

<sup>10</sup> The Internal Revenue Manual serves as the IRS' official source to communicate security guidance to employees and contractors.

<sup>11</sup> *Standard Database Security Configurations Are Adequate, Although Much Work Is Needed to Ensure Proper Implementation* (Reference Number 2007-20-129, dated August 22, 2007).

<sup>12</sup> *Effectiveness of Access Controls Over System Administrator User Accounts Can Be Improved* (Reference Number 2007-20-161, dated September 19, 2007).



---

## *Improvements Are Needed to the Information Security Program Governance Process*

---

addition, the Cybersecurity organization maintains security updates or interim guidance on a different webpage, thus increasing the risk that recently developed security controls will be overlooked.

The confusion caused by maintaining guidance in multiple locations and the difficulty in finding the guidance on the web site increase the likelihood that employees and contractors could unknowingly create security weaknesses that result in security breaches. We believe the current process used to provide security guidance needs to be streamlined.

### ***Recommendations***

The Associate Chief Information Officer, Cybersecurity, should:

**Recommendation 6:** Coordinate with other executives in the Modernization and Information Technology Services organization to include complete NIST-compliant security guidance regarding the system development life cycle and capital planning. Coordination is also required with the Chief, Agency-Wide Shared Services, to develop complete security guidance regarding the acquisition of services.

**Management's Response:** IRS management agreed with the recommendation. The Cybersecurity organization will work with other organizations in the Modernization and Information Technology Services organization and the business units to include NIST-compliant security guidance in both the system development life cycle and capital planning processes. It will work with the Agency-Wide Shared Services organization to develop appropriate security contractual guidance and processes for acquisition of information technology and services.

**Recommendation 7:** Improve the Cybersecurity organization Intranet web site to facilitate easy access to current information security guidance. The web site should provide direct links to NIST guidance.

**Management's Response:** IRS management agreed with the recommendation. The Cybersecurity organization is redesigning its web site to give internal and external customers a tool that will be focused on sharing security information and services. It will add a direct link to NIST guidance as a new feature of the web site redesign.

**Recommendation 8:** Develop a system to notify employees and contractors of changes in security guidance.

**Management's Response:** IRS management agreed with the recommendation. The Cybersecurity organization will distribute and report changes in security guidance through the distribution list of the Security Services and Privacy Executive Steering Committee where all IRS offices are represented. The details in the guidance will specify applicability to contractors. The Cybersecurity organization will also work with the



*Improvements Are Needed to the Information Security Program  
Governance Process*

---

Agency-Wide Shared Services organization Procurement Office and with all IRS offices to ensure distribution of the security guidance to IRS contractors through the Contracting Officer's Technical Representatives.



## Appendix I

### *Detailed Objective, Scope, and Methodology*

The overall objective of this review was to determine whether the IRS monitored compliance with security policies and procedures and developed sufficient information security guidance. To accomplish this objective, we:

- I. Determined whether the Cybersecurity organization had implemented adequate processes to ensure agency-wide compliance with security guidance.
  - A. Determined whether the Cybersecurity organization had defined security roles and responsibilities for key leadership positions specified in the NIST<sup>1</sup> *Information Security Handbook* (Special Publication 800-100) to promote, issue, and enforce information security guidance within the IRS. We compared NIST standards to the roles and responsibilities set forth in the Internal Revenue Manual.<sup>2</sup>
  - B. Determined what actions had been taken by the Cybersecurity organization to ensure compliance with security controls and procedures.
  - C. Reviewed actions taken to ensure that security guidance issued by the Cybersecurity organization had been followed and determined whether those actions were effective.
- II. Determined whether the Cybersecurity organization had developed sufficient and timely guidance to ensure an effective information security governance program. We reviewed NIST Special Publication 800-100, Treasury Information Technology Security Program Directive 85-01, the Internal Revenue Manual, and other Federal Government guidance and obtained information on security program standards.
  - A. Determined whether the Cybersecurity organization had developed adequate procedures for security areas specified in NIST Special Publication 800-100 and compared NIST standards to Cybersecurity organization information security guidance in the Internal Revenue Manual.
  - B. Determined who was responsible for issuing security controls and procedures in the Cybersecurity organization and how long it took for security guidance to be issued.

---

<sup>1</sup> The NIST, under the Department of Commerce, is responsible for developing standards and guidelines for providing adequate information security for all Federal Government agency operations and assets.

<sup>2</sup> The Internal Revenue Manual serves as the IRS' official source to communicate security guidance to employees and contractors.



*Improvements Are Needed to the Information Security Program  
Governance Process*

---

**Appendix II**

*Major Contributors to This Report*

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)  
Stephen Mullins, Director  
Michelle Griffin, Audit Manager  
Cari Fogle, Senior Auditor  
Jody Kitazono, Senior Auditor  
Abraham Millado, Senior Auditor  
Stasha Smith, Senior Auditor



---

*Improvements Are Needed to the Information Security Program  
Governance Process*

---

**Appendix III**

*Report Distribution List*

Acting Commissioner C  
Office of the Commissioner – Attn: Acting Chief of Staff C  
Deputy Commissioner for Operations Support OS  
Chief, Agency-Wide Shared Services OS:A  
Director, Program Oversight OS:CIO:SM:PO  
Chief Counsel CC  
National Taxpayer Advocate TA  
Director, Office of Legislative Affairs CL:LA  
Director, Office of Program Evaluation and Risk Analysis RAS:O  
Office of Internal Controls OS:CFO:CPIC:IC  
Audit Liaisons:  
    Chief, Agency-Wide Shared Services OS:A  
    Chief Information Officer OS:CIO



*Improvements Are Needed to the Information Security Program  
Governance Process*

**Appendix IV**

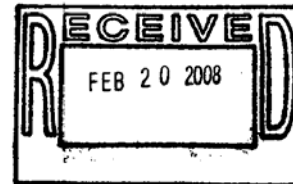
*Management's Response to the Draft Report*



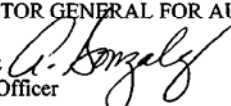
CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY  
INTERNAL REVENUE SERVICE  
WASHINGTON, D. C. 20224

February 15, 2008



MEMORANDUM FOR MICHAEL R. PHILLIPS  
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Arthur L. Gonzalez   
Chief Information Officer

SUBJECT: Draft Audit Report – Management Response to Draft Audit Report –  
Improvements Are Needed to the Information Security Program  
Governance Process (Audit #200620026) (i-trak #2008-32585)

Thank you for the opportunity to review and respond to the draft audit report. We take our security posture and our responsibility for developing an effective security governance process that complies with federal government standards very seriously.

Crucial to effective governance is developing and documenting adequate security guidance as the primary means to communicate IRS management's requirements. The National Institute for Standards and Technology (NIST) Special Publication 800-100 covers 12 key aspects of information security that information security managers are expected to implement and oversee in their respective organizations. The IRS Office of Cybersecurity, Modernization and Information Technology Services, is responsible for developing the security guidance for the 12 security areas covered by NIST. We appreciate that your report acknowledges that Cybersecurity has made significant progress in developing effective information security guidance that meets NIST standards for 9 of the 12 security areas. We are aggressively pursuing initiatives to ensure existing guidance in the remaining three security areas is current and complete.

As part of our response to the audit findings, we are reviewing our annual testing activities of security controls. We are working with Treasury Department staff to clarify security controls testing guidance and obtain agreement with Treasury and your office on the scope and methodology for future annual security controls testing activities.

We agree with, and will implement, all eight report recommendations. The attachment to this memo provides our detailed corrective action plans to address the recommendations.

Thank you for your continued support and guidance. We look forward to working with TIGTA in the future on this important area. If you have any questions, please contact me at (202) 622-6800 or Perry Robinett, Director, Program Oversight Coordination, at (202) 283-6283.

Attachment





---

*Improvements Are Needed to the Information Security Program Governance Process*

---

**Attachment**

**Management Response to Draft Audit Report – Improvements Are Needed to the Information Security Program Governance Process (Audit # 200620026) (i-trak # 2008-32585)**

---

**RECOMMENDATION #1:** The Chief Information Officer, through the Security Services and Privacy Executive Steering Committee, should require system owners to regularly report to the Committee on progress in addressing Plan of Action and Milestones (POA&M) items. On a sample basis, the Committee should require system owners to provide documentation to demonstrate that corrective actions were adequate to resolve weaknesses.

**CORRECTIVE ACTION TO RECOMMENDATION #1:** We agree with this recommendation. Cybersecurity, in Modernization and Information Technology Services (MITS), has developed a Federal Information Security Management Act (FISMA) Dashboard to provide the current status of each FISMA activity, including progress on Plan of Action and Milestones (POA&M) at every Security Services and Privacy Executive Steering Committee meeting. Cybersecurity will give additional focus to POA&Ms by adding an agenda item to the meeting for business units to report the progress on their open POA&M items.

MITS Cybersecurity will then sample closed POA&M items and review the evidence on the Treasury system Trusted Agent FISMA to validate the closure. Cybersecurity will present the results of this verification process to the Security Services and Privacy Executive Steering Committee.

**IMPLEMENTATION DATE:** December 1, 2008

**RESPONSIBLE OFFICIAL:** Associate Chief Information Officer, Cybersecurity

**CORRECTIVE ACTION MONITORING PLAN:** Corrective actions are maintained in the Joint Audit Management Enterprise System (JAMES) and monitored monthly until completion.

**RECOMMENDATION #2:** The Chief Information Officer, through the Security Services and Privacy Executive Steering Committee, should require the Cybersecurity organization to improve the verification of compliance with standard configurations by:

- Executing compliance checker tools and vulnerability scans more frequently than quarterly. Results should be provided to the Chief Information Officer and the Security Services and Privacy Executive Steering Committee.
- Extending scanning to evaluate database security.
- Including the results of scans in POA&Ms until issues are resolved.

**CORRECTIVE ACTION TO RECOMMENDATION #2:** We agree with this recommendation. For security configuration compliance and vulnerability management, Cybersecurity will conduct scans once every six weeks to identify noncompliance with IRS standards. In addition, Cybersecurity will extend scanning to evaluate database security and



---

*Improvements Are Needed to the Information Security Program Governance Process*

---

**Attachment**

**Management Response to Draft Audit Report – Improvements Are Needed to the Information Security Program Governance Process (Audit # 200620026) (i-trak # 2008-32585)**

---

report scan results to both the Chief Information Officer and the Security Services and Privacy Executive Steering Committee, and track in POA&Ms until issues are resolved.

**IMPLEMENTATION DATE:** January 1, 2009

**RESPONSIBLE OFFICIAL:** Associate Chief Information Officer, Cybersecurity

**CORRECTIVE ACTION MONITORING PLAN:** Corrective actions are maintained in the Joint Audit Management Enterprise System (JAMES) and monitored monthly until completion.

**RECOMMENDATION #3:** The Chief Information Officer, through the Security Services and Privacy Executive Steering Committee, should analyze the incidents reported to the Computer Security Incident Response Center, to identify common or systemic underlying weaknesses that contributed to these incidents, and track corrective actions in the appropriate POA&M.

**CORRECTIVE ACTION TO RECOMMENDATION #3:** We agree with this recommendation. The Computer Security Incident Response Center, Cybersecurity, based on reported incidents, will prepare quarterly trend reports that identify common or systemic underlying weaknesses that contribute to these incidents, and incorporate and track these weaknesses in the appropriate POA&Ms until resolved. That office will provide this information to the Security Services and Privacy Executive Steering Committee.

**IMPLEMENTATION DATE:** October 1, 2008

**RESPONSIBLE OFFICIAL:** Associate Chief Information Officer, Cybersecurity

**CORRECTIVE ACTION MONITORING PLAN:** Corrective actions are maintained in the Joint Audit Management Enterprise System (JAMES) and monitored monthly until completion.

**RECOMMENDATION #4:** The Chief Information Officer, through the Security Services and Privacy Executive Steering Committee, should ensure system owners prepare continuous monitoring plans that implement annual testing of system controls compliant with NIST Special Publications 800-53 and 800-53A. The testing should include closed POA&M items and other volatile controls. On a sample basis, the Committee should ensure that adequate documentation is maintained to support the test results and closure of POA&M items.

**CORRECTIVE ACTION TO RECOMMENDATION #4:** We agree with this recommendation. The IRS enterprise continuous monitoring approach requires that system owners prepare Continuous Monitoring Plans in compliance with NIST 800-53 and 800-53A. This approach requires that testing include closed POA&M items and other volatile controls. The Business Owner will include the closed POA&M items in its annual testing. The business



---

*Improvements Are Needed to the Information Security Program Governance Process*

---

**Attachment**

**Management Response to Draft Audit Report – Improvements Are Needed to the Information Security Program Governance Process (Audit # 200620026) (i-trak # 2008-32585)**

---

owner is responsible for planning and performing testing, documenting the results, and collecting and posting the evidence to the Trusted Agent FISMA for tracking and reporting purposes.

MITS Cybersecurity will develop a process to validate that the system owners are following the Enterprise Continuous Monitoring approach. This approach includes sampling and validating closed POA&M items by evaluating the test results and evidence on Trusted Agent FISMA and presenting the results of that review to the Security Services and Privacy Executive Steering Committee.

**IMPLEMENTATION DATE:** October 1, 2009

**RESPONSIBLE OFFICIAL:** Associate Chief Information Officer, Cybersecurity

**CORRECTIVE ACTION MONITORING PLAN:** Corrective actions are maintained in the Joint Audit Management Enterprise System (JAMES) and monitored monthly until completion.

**RECOMMENDATION #5:** The Chief Information Officer, through the Security Services and Privacy Executive Steering Committee, should develop quantifiable security metrics based on IRS information security goals and objectives. The Cybersecurity organization should analyze anomalies for root causes and report its results regularly to the Committee.

**CORRECTIVE ACTION TO RECOMMENDATION #5:** We agree with this recommendation. MITS Cybersecurity will develop a process and collect quantifiable security metrics based on the IRS's security goals and objectives. Cybersecurity will analyze these metrics for the root causes of anomalies and report the metrics and results of the analyses to the Security Services and Privacy Executive Steering Committee.

**IMPLEMENTATION DATE:** December 1, 2008

**RESPONSIBLE OFFICIAL:** Associate Chief Information Officer, Cybersecurity

**CORRECTIVE ACTION MONITORING PLAN:** Cybersecurity will present a briefing on the progress of this corrective action at the Policy and Programs Operational Review.

**RECOMMENDATION #6:** The Associate Chief Information Officer, Cybersecurity, should coordinate with other executives in the Modernization and Information Technology Services organization to include complete NIST-compliant security guidance regarding the system development life cycle and capital planning. Coordination is also required with the Chief, Agency-Wide Shared Services, to develop complete security guidance regarding the acquisition of services.



---

*Improvements Are Needed to the Information Security Program  
Governance Process*

---

**Attachment**

**Management Response to Draft Audit Report – Improvements Are Needed to the  
Information Security Program Governance Process (Audit # 200620026)  
(i-trak # 2008-32585)**

---

**CORRECTIVE ACTION TO RECOMMENDATION #6:** We agree with this recommendation. MITS Cybersecurity will work with other organizations in MITS and the Business Units to include NIST-compliant security guidance in both the system development life cycle and capital planning process. MITS Cybersecurity will work with Agency-Wide Shared Services Procurement to develop appropriate security contractual guidance and processes for acquisition of information technology (IT) and IT services.

**IMPLEMENTATION DATE:** March 1, 2009

**RESPONSIBLE OFFICIAL:** Associate Chief Information Officer, Cybersecurity

**CORRECTIVE ACTION MONITORING PLAN:** Corrective actions are maintained in the Joint Audit Management Enterprise System (JAMES) and monitored monthly until completion.

**RECOMMENDATION #7:** The Associate Chief Information Officer, Cybersecurity, should: Improve the Cybersecurity organization Intranet web site to facilitate easy access to current information security guidance. The web site should provide direct links to NIST guidance.

**CORRECTIVE ACTION TO RECOMMENDATION #7:** We agree with this recommendation. Communications & Support Services Office, Cybersecurity, is redesigning the Cybersecurity web site to give internal and external customers a tool that will be focused on sharing security information and resources. It will add a direct link to NIST guidance as a new feature of the web site redesign.

**IMPLEMENTATION DATE:** September 1, 2008

**RESPONSIBLE OFFICIAL:** Associate Chief Information Officer, Cybersecurity

**CORRECTIVE ACTION MONITORING PLAN:** Corrective actions are maintained in the Joint Audit Management Enterprise System (JAMES) and monitored monthly until completion.

**RECOMMENDATION #8:** The Associate Chief Information Officer, Cybersecurity, should develop a system to notify employees and contractors of changes in security guidance.

**CORRECTIVE ACTION TO RECOMMENDATION #8:** We agree with this recommendation. MITS Cybersecurity will distribute and report changes in security guidance through the distribution list of the Security Services and Privacy Executive Steering Committee where all IRS offices are represented. The details in the guidance will specify applicability to contractors. Cybersecurity will also work with Agency-Wide Shared Services Procurement, and



---

*Improvements Are Needed to the Information Security Program  
Governance Process*

---

**Attachment**

**Management Response to Draft Audit Report – Improvements Are Needed to the  
Information Security Program Governance Process (Audit # 200620026)  
(i-trak # 2008-32585)**

---

with all IRS offices to ensure the distribution of the security guidance to IRS contractors through the Contracting Officer Technical Representatives (COTRs).

**IMPLEMENTATION DATE:** December 1, 2008

**RESPONSIBLE OFFICIAL:** Associate Chief Information Officer, Cybersecurity

**CORRECTIVE ACTION MONITORING PLAN:** Corrective actions are maintained in the Joint Audit Management Enterprise System (JAMES) and monitored monthly until completion.