Treasury Inspector General for Tax Administration – Federal Information Security Management Act Report for Fiscal Year 2012

September 28, 2012

Reference Number: 2012-20-114

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.

Phone Number | 202-622-6500
E-mail Address | TIGTACommunications@tigta.treas.gov
Website | http://www.tigta.gov

TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION – FEDERAL INFORMATION SECURITY MANAGEMENT ACT REPORT FOR FISCAL YEAR 2012

Highlights

Report issued on September 28, 2012

Highlights of Report Number: 2012-20-114 to the Department of the Treasury, Office of the Inspector General, Assistant Inspector General for Audit.

IMPACT ON TAXPAYERS

The IRS collects and maintains a significant amount of personal and financial information on each taxpayer. The IRS also relies extensively on computerized systems to support its responsibilities in collecting taxes, processing tax returns, and enforcing the Federal tax laws. As custodians of taxpayer information, the IRS has an obligation to protect the confidentiality of this sensitive information against unauthorized access or loss. Otherwise, taxpayers could be exposed to invasion of privacy and financial loss or damage from identity theft or other financial crimes.

WHY TIGTA DID THE AUDIT

The Federal Information Security Management Act (FISMA) was enacted to strengthen the security of information and systems within Federal agencies. As part of this legislation, the Offices of Inspectors General are required to perform an annual independent evaluation of each Federal agency's information security programs and practices. This report reflects TIGTA's independent evaluation of the status of the IRS's information security program for Fiscal Year 2012.

WHAT TIGTA FOUND

Based on our Fiscal Year 2012 FISMA evaluation, TIGTA found that the IRS's information security program was generally compliant with the FISMA requirements. Specifically, TIGTA determined that the following eight program areas met the level of performance specified by the Department of Homeland Security's *Fiscal Year 2012 Inspector General FISMA Reporting Metrics*:

- Continuous monitoring management.
- Incident response and reporting.
- Risk management.
- Plan of action and milestones.
- Remote access management.
- Contingency planning.
- Contractor systems.
- Security capital planning.

However, TIGTA determined that the following program areas did not meet the level of performance specified by the Department of Homeland Security's *Fiscal Year 2012 Inspector General FISMA Reporting Metrics* as a result of specific program attributes that were missing or other conditions identified that reduced program effectiveness:

- Configuration management.
- Identity and access management.
- Security training.

WHAT TIGTA RECOMMENDED

TIGTA does not include recommendations as part of its annual FISMA evaluation and reports only on the level of performance achieved by the IRS using the guidelines issued by the Department of Homeland Security for the applicable FISMA evaluation period.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 28, 2012

MEMORANDUM FOR ASSISTANT INSPECTOR GENERAL FOR AUDIT
OFFICE OF THE INSPECTOR GENERAL
DEPARTMENT OF THE TREASURY

FROM: Michael E. McKenney
Acting Deputy Inspector General for Audit

SUBJECT: Treasury Inspector General for Tax Administration – Federal Information Security Management Act Report for Fiscal Year 2012 (Audit # 201220001)

This report presents the results of the Treasury Inspector General for Tax Administration's Federal Information Security Management Act[1] evaluation for Fiscal Year 2012. The Act requires the Offices of Inspectors General to perform an annual independent evaluation of each Federal agency's information security program and practices. This report reflects our independent evaluation of the Internal Revenue Service's (IRS) information security program and practices for the period under review.

The report was forwarded to the Treasury Inspector General for consolidation into a report issued to the Department of the Treasury Chief Information Officer. Copies of this report are also being sent to the IRS managers affected by the report results.

Please contact me at (202) 622-6510 if you have questions or Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services), at (202) 622-5894.

[1] Title III of the E-Government Act of 2002, Pub. L. No. 107-374, 116 Stat. 2899.

Table of Contents

Background ..... Page 1

Results of Review ..... Page 2

The Internal Revenue Service's Information Security Program Generally Complies With the Federal Information Security Management Act, but Improvements Are Needed ..... Page 2

Appendices

Appendix I – Fiscal Year 2012 Reporting Metrics ..... Page 16

Appendix II – Major Contributors to This Report ..... Page 30

Appendix III – Report Distribution List ..... Page 31

Appendix IV – Treasury Inspector General for Tax Administration Information Technology Security-Related Reports Issued During the Fiscal Year 2012 Evaluation Period ..... Page 32

Appendix V – Glossary of Terms ..... Page 33

Abbreviations

AP	Administrative Priority
Base	Baseline Question
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CM	Continuous Monitoring
CMWG	Continuous Monitoring Working Group
DAA	Designated Accrediting Authority
DHS	Department of Homeland Security
DMZ	Demilitarized Zone
ECMS	Enterprise Configuration Management System
FCD1	Federal Continuity Directive 1
FDCC	Federal Desktop Core Configuration
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GAO	Government Accountability Office
GSS	General Support System
HSPD-12	Homeland Security Presidential Directive-12
IP	Internet Protocol
IRS	Internal Revenue Service
IT	Information Technology
KFM	Key FISMA Metric
MOU	Memorandum of Understanding

NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones
SCAP	Security Content Automation Protocol
SP	Special Publication
TIGTA	Treasury Inspector General for Tax Administration
US-CERT	United States Computer Emergency Response Team
USG	U.S. Government
USGCB	United States Government Configuration Baseline

Background

The Internal Revenue Service (IRS) collects and maintains a significant amount of personal and financial information on each taxpayer. The IRS also relies extensively on computerized systems to support its responsibilities in collecting taxes, processing tax returns, and enforcing Federal tax laws. As custodians of taxpayer information, the IRS has an obligation to protect the confidentiality of this sensitive information against unauthorized access or loss. Otherwise, taxpayers could be exposed to invasion of privacy and financial loss or damage from identity theft or other financial crimes.

The Federal Information Security Management Act (FISMA) of 2002[1] was enacted to strengthen the security of information and systems within Federal agencies. Under the FISMA, agency heads are responsible for providing information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. Agency heads are also responsible for complying with the requirements of the FISMA, related Office of Management and Budget (OMB) policies, and National Institute of Standards and Technology (NIST) procedures, standards, and guidelines.

As part of this legislation, each Federal Government agency is required to report annually to the OMB on the adequacy and effectiveness of its information security program and practices and compliance with the FISMA. In addition, the FISMA requires the agencies to have an annual independent evaluation of their information security programs and practices performed by the agency Inspector General or an independent external auditor as determined by the Inspector General.[2] The OMB uses the information from the agencies and independent evaluations in its FISMA oversight capacity to assess agency-specific and Federal Government-wide security performance, develop its annual security report to Congress, and assist in improving and maintaining adequate agency security performance.

We based our evaluation of the IRS on the Department of Homeland Security's (DHS) *Fiscal Year (FY) 2012 Inspector General FISMA Reporting Metrics* issued on March 6, 2012. These reporting metrics specified the security program areas for the Inspectors General to evaluate and listed specific attributes that each security program area should include, as shown in Appendix I. Major contributors to this report are listed in Appendix II.

[1] Title III of the E-Government Act of 2002, Pub. L. No. 107-374, 116 Stat. 2899.
[2] The FISMA evaluation period for the Department of the Treasury is July 1, 2011, through June 30, 2012. All subsequent references to 2012 refer to the FISMA evaluation period.

Results of Review

The Internal Revenue Service's Information Security Program Generally Complies With the Federal Information Security Management Act, but Improvements Are Needed

The DHS *FY 2012 Inspector General FISMA Reporting Metrics* specified 11 information security program areas and a total of 96 attributes within the 11 areas for the Inspectors General to evaluate and determine whether agencies had established and maintained an information security program that was generally consistent with the NIST and OMB's FISMA requirements. The 11 information security program areas are as follows:

- Continuous monitoring management.
- Configuration management.
- Identity and access management.
- Incident response and reporting.
- Risk management.
- Security training.
- Plan of action and milestones.
- Remote access management.
- Contingency planning.
- Contractor systems.
- Security capital planning.

To complete our FISMA evaluation, we reviewed a representative sample of 10 major IRS information systems. For each system in the sample, we assessed the quality of the security assessment and authorization process, the annual testing of controls for continuous monitoring, the testing of information technology contingency plans, and the quality of the plan of action and milestones process. In addition, we evaluated the IRS's processes over configuration management, identity and access management, incident response and reporting, security training, remote access management, contractor systems, and security capital planning. During the FY 2012 FISMA evaluation period, we also completed nine audits, as shown in Appendix IV, which evaluated various aspects of information security at the IRS. We considered the results of these audits in our evaluation, as well as results from ongoing audits for which draft reports were issued to the IRS by August 10, 2012.

Based on our FY 2012 FISMA evaluation, we determined that the IRS's information security program was compliant with the FISMA requirements and met the level of performance for eight of the 11 program areas as specified by the DHS's *FY 2012 Inspector General FISMA Reporting Metrics*. However, we also noted that improvements were needed in the remaining three program areas. We determined that these three program areas did not meet the level of performance specified by the DHS's *FY 2012 Inspector General FISMA Reporting Metrics* as a result of specific program attributes that were missing or other conditions that we identified which reduced program effectiveness. The three areas needing improvement are as follows:

- Configuration management.
- Identity and access management.
- Security training.

Configuration Management

Configuration management comprises a collection of activities focused on establishing and maintaining the integrity of products and systems through control of the processes for initializing, changing, and monitoring the configurations of those products and systems. Security-focused configuration management is the management and control of secure configurations for an information system to enable security and facilitate the management of risk. Effective configuration management of information systems requires the integration of the management of secure configurations into the organizational configuration management process or processes.

In order to secure both software and hardware, agencies must develop and implement standard configuration baselines that prevent or minimize exploitable system vulnerabilities. The OMB requires all Windows 7, XP, and Vista workstations to conform to the U.S. Government Configuration Baseline. Furthermore, the NIST has created a repository of secure baselines for a wide variety of operating systems and devices. Agencies must also develop and implement sufficient patch management processes, which is a component of configuration management. Any significant delays in patching software with critical vulnerabilities provide ample opportunity for persistent attackers to gain control over the vulnerable computers and get access to the sensitive data they may contain.

The IRS has not fully implemented the following seven configuration management attributes specified by the DHS metrics:

2.1.3. Assessing for compliance with baseline configurations.

2.1.5. For Windows-based components, Federal Desktop Core Configuration (FDCC)/U.S. Government Configuration Baseline (USGCB) secure configuration settings fully implemented and any deviations from FDCC/USGCB baseline settings fully documented.

2.1.6. Documented proposed or actual changes to hardware and software configurations.

2.1.7. Process for timely and secure installation of software patches.

2.1.8. Software assessing (scanning) capabilities are fully implemented.

2.1.9. Configuration-related vulnerabilities, including scan findings, have been remediated in a timely manner, as specified in organization policy or standards.

2.1.10. Patch management process is fully developed, as specified in organization policy or standards.

2.1.3. Assessing for compliance with baseline configurations.

The IRS is still in the process of implementing tools compliant with the Security Content Automation Protocol (SCAP)[3] to perform security configuration assessments for Windows and UNIX systems. Agencies are required to use SCAP-validated tools, as specified by the NIST, to continuously monitor the security configurations of their information technology assets as part of compliance with the FISMA.

In April 2008, the IRS formally kicked off an initiative to implement the Security Compliance Posture Monitoring and Reporting tool, an enterprise tool that would utilize the NIST-defined protocol. When in production, the Security Compliance Posture Monitoring and Reporting tool would provide the IRS with the ability to monitor, measure, and manage FISMA security compliance of its Windows and UNIX servers enterprise-wide. Also, it would allow the IRS to retire the Windows and UNIX policy checker programs, which are not SCAP-compliant. However, the IRS has not yet rolled out the Security Compliance Posture Monitoring and Reporting tool.

Also, in September 2011, the Treasury Inspector General for Tax Administration (TIGTA) reported[4] that automated security configuration scans of IRS mainframe databases were not conducted. The Internal Revenue Manual required monthly automated security configuration scans of all operating and database systems. However, the mainframe policy checker does not test configuration compliance for databases that reside on mainframes. The IRS agreed to implement automated security configuration scanning on mainframe databases by March 1, 2013.

[3] The SCAP is a suite of specifications that standardize the format and nomenclature by which security software products communicate software flaw and security configuration information. SCAP is designed to organize, express, and measure security-related information in standardized ways, as well as related reference data, such as identifiers for post-compilation software flaws and security configuration issues. SCAP can be used to maintain the security of enterprise systems, such as automatically verifying the installation of patches, checking system security configuration settings, and examining systems for signs of compromise.

[4] TIGTA Ref. No. 2011-20-099, *The Mainframe Databases Reviewed Met Security Requirements; However, Automated Security Scans Were Not Performed* (Sept. 2011).

The IRS has deployed a SCAP-compliant tool (called the SCAP Compliance Checker) for monitoring Federal Desktop Core Configuration compliance on workstations. However, since February 2010, the IRS has been in the process of implementing additional tools for monitoring workstation compliance, called the Treasury Enhanced Security Initiative. The IRS believes the Treasury Enhanced Security Initiative is needed because of the features it has that the SCAP Compliance Checker does not have, including its ability to:

- Discover all assets on the IRS network.
- Identify rogue computers.
- Monitor administrative access privileges.
- Identify noncompliant security configurations for specific workstations.
- Prioritize highest risk systems for timely remediation.
- Automate remediation of some misconfigurations.

However, the Treasury Enhanced Security Initiative has experienced several delays due to the need for infrastructure upgrades and additional server resources, the IRS placing higher priorities on development of other systems, and filing season moratoriums.

2.1.5. For Windows-based components, FDCC/USGCB secure configuration settings fully implemented and any deviations from FDCC/USGCB baseline settings fully documented.

The IRS has not yet fully documented Windows 7 FDCC/USGCB deviations. The User and Network Services organization indicated that it is currently working with stakeholders to identify and document all Windows 7 settings that do not comply with the Internal Revenue Manual or USGCB.

2.1.6. Documented proposed or actual changes to hardware and software configurations.

The IRS had not yet fully implemented configuration and change management controls to ensure that proposed or actual changes to hardware and software configurations are documented. During FY 2012, the Enterprise Services organization was in the process of implementing the Enterprise Configuration Management System (ECMS) to provide an enterprise solution for configuration and change management. The goal of the ECMS is to provide the IRS the capability to automate the configuration management process, enhance and improve the current change management process, provide a platform for the consolidation of change boards, provide a detailed change analysis capability, and support the adoption of robust configuration management and validation.

The ECMS briefing from the Enterprise Services Configuration and Change Management office cites a number of issues with IRS configuration and change management processes, including:

- A number of organizational change management processes are in place, without a clear understanding on how they link back to the "umbrella" configuration and change management standards.
    - Duplicative steps exist in many of the change management processes.
    - Inconsistent integration/coordination exists across processes.
- There is limited enforcement of configuration and change management standards to date.
- Multiple configuration control boards are in place, without a clear definition of what the hand-offs are between them.
- Configuration items do not always have an owner.
- No clear process hand-offs are defined between configuration management, change management, release management, and other service management processes.
- Organizations do not always have a clear understanding of Configuration and Change Management office staff roles.
- Many organizations do not have a clear understanding of what configuration and change management are and what steps they should be following to perform the related processes.
- Configuration and change management standards applied to organizationally owned tools are sometimes "lost in translation."
- The level of effort required across varied tools and procedures involved in performing configuration management activities is not clear, making it difficult to assign resources.

In July 2012, the Enterprise Services organization deployed the initial release of the ECMS. The ECMS includes a configuration item discovery tool, called the Discovery and Dependency Mapping Advanced tool, for the purpose of establishing a central repository of configuration items for which changes to configuration settings will need to be managed. The Enterprise Services organization plans for the full implementation of the ECMS to occur in FY 2014.

2.1.7. Process for timely and secure installation of software patches.

During the FY 2012 FISMA evaluation period, the TIGTA concluded fieldwork on an audit to evaluate the IRS's enterprise-wide patch management process.[5] The TIGTA identified that critical patches continue to be missing or are installed in an untimely manner. The IRS's own patch monitoring reports continue to report unpatched or untimely patched computers. For example, an IRS-wide patch monitoring report for Windows servers, called the Associate Chief

[5] TIGTA, Ref. No. 2012-20-012, *An Enterprise Approach Is Needed to Address the Security Risk of Unpatched Computers* (Sep. 2012).

Information Officer Monthly Critical Patch Report, showed the IRS's overall patch compliance rate for critical patches averaged 88 percent in March 2012, ranging from a low of 63 percent to a high of 88 percent for the six-month period of October 2011 to March 2012. The March 2012 report showed that 7,329 potential vulnerabilities remain on IRS servers because 23 critical patches had not been installed on servers that need them; some of these patches had been released as far back as April 2011. These vulnerabilities could potentially be exploited to gain unauthorized access to information, disrupt operations, or launch attacks against other systems.

In addition, the IRS informed us that patching is still manual for the majority of its UNIX operating systems and is not in accordance with patch frequencies required by the Internal Revenue Manual. The Enterprise Operations organization is currently testing a process for automating patching on its UNIX servers.

IRS patch management policy did not provide clear expectations for when patches must be installed. In addition, the IRS has no mechanism to enforce timely patching or to hold system owners accountable for ensuring that their systems are timely patched or that they formally accept the risk of not patching systems timely. By not installing security patches in a timely fashion, the IRS increases the risk that known vulnerabilities in its systems may be exploited.

In March 2012, the Government Accountability Office (GAO) also reported[6] that the IRS did not always apply critical patches or ensure versions of its operating system were still supported by the vendor.

2.1.8. Software assessing (scanning) capabilities are fully implemented.

The IRS's software assessing (scanning) capabilities are not yet fully implemented. The IRS Organizational Common Controls Security Plan, Version 1, dated June 28, 2012, stated that the required vulnerability scanning control was not in place at the IRS organizational level and that the IRS Cybersecurity organization is still in the process of coordinating with information system owners to implement vulnerability scanning enterprise-wide. It also stated that, for vulnerability scans the IRS did conduct, analysis of the scans were not being performed by the system owners. In addition, it stated that the IRS has not yet deployed an automated mechanism to detect the presence of unauthorized software on IRS information systems.

In June 2012, the TIGTA reported[7] that the IRS had not implemented or enforced enterprise-wide procedures for monitoring and remediating weaknesses reported by nCircle scans. These scans help to identify what details about the information system are discoverable by adversaries and provide an associated risk level/score. During FY 2012, the IRS Cybersecurity organization was in the process of developing enterprise-wide standard operating

[6] GAO, GAO-12-393, *IRS Needs to Further Enhance Internal Control Over Financial Reporting and Taxpayer Data* (Mar. 2012).
[7] TIGTA, Ref. No. 2012-20-063, *Enterprise-Level Oversight Is Needed to Ensure Adherence to Windows Server Security Policies* (June 2012).

procedures for reviewing and analyzing the results of vulnerability scans and educating system owners on how to prioritize and resolve the identified weaknesses.

In September 2011, the TIGTA reported[8] that four individuals had installed and used personal unauthorized wireless devices on their laptops to connect to the IRS network. The TIGTA recommended that the IRS implement automated nationwide network scans for unauthorized wireless activity, devices, and software and improve processes to handle incidents of noncompliance with IRS security policy so that when unauthorized wireless activity is identified, subsequent investigations and disciplinary actions are effective. The IRS plans to complete the corrective action by September 28, 2012.

Additionally, our review of 10 sample systems' System Security Plans revealed that vulnerability scans were not being conducted in accordance with the IRS's defined frequency and process for the three General Support System's (GSS) in our sample.

2.1.9. Configuration-related vulnerabilities, including scan findings, have been remediated in a timely manner, as specified in organization policy or standards.

In June 2012, the TIGTA reported[9] that monthly scanning results were not consistently being used to correct improper settings on Windows servers in a timely manner; rather, security vulnerabilities of high, medium, and low risk levels were repeatedly reported on Windows Policy Checker reports for two or three consecutive months. During FY 2012, the Cybersecurity organization issued standard operating procedures for the monitoring and remediation of weaknesses reported by the Windows server configuration scans to all IRS staff administering Windows servers. The document stated that the Cybersecurity organization staff will work with the system administrators, application owners, and project offices to maintain a 100-percent compliance level on all Windows servers across all IRS organizations.

2.1.10. Patch management process is fully developed, as specified in organization policy or standards.

During the FY 2012 FISMA evaluation period, the TIGTA concluded fieldwork on an audit to evaluate the IRS's enterprise-wide patch management process.[10] The TIGTA identified that, although IRS policy requires the IRS to establish an enterprise-level group with responsibility for patch management, no enterprise-level group exists. Due to the lack of enterprise-level oversight and leadership, the IRS has not yet implemented key elements of its patch management policies and procedures that are needed to ensure all IRS systems are patched timely and operating

[8] TIGTA, Ref. No. 2011-20-101, *Security Controls Over Wireless Technology Were Generally in Place; However, Further Actions Can Improve Security* (Sept. 2011).
[9] TIGTA, Ref. No. 2012-20-063, *Enterprise-Level Oversight Is Needed to Ensure Adherence to Windows Server Security Policies* (June 2012).
[10] TIGTA, Ref. No. 2012-20-012, *An Enterprise Approach Is Needed to Address the Security Risk of Unpatched Computers* (Sep. 2012).

securely. Specifically, the IRS has not:

- Completed the implementation of an accurate and complete inventory of its information technology assets, which is critical for ensuring that patches are identified and applied timely for all types of operating systems and software used within its environment.
- Implemented patch policy and monitoring processes to ensure patches are applied timely enterprise-wide.
- Implemented controls to ensure that unsupported operating systems are not putting the IRS at risk.

IRS processes to monitor the installation of required patches need improvement. The IRS's current monitoring processes are not sufficient to ensure that vulnerabilities resulting from unpatched systems are successfully and timely remediated. The IRS depends on the various IRS organizations that manage their own computers to frequently self-report patching data from their organization-level patch monitoring reports. This effort is labor intensive and results in incomplete and unverified patch data. For example, in March 2012, the IRS Information Technology organization reported that it had not received percentage data for 14 consecutive months from non-Information Technology managed Windows workstations needing critical patches, which it needed to track patch metrics in its Information Technology Internal Dashboard. Further, the IRS had not established patch performance metrics in terms of setting compliance rate goals and measuring them on a monthly basis to ensure IRS organizations are complying with security patch policy.

2.2. Please provide any additional information on the effectiveness of the organization's configuration management program that was not noted in the questions above.

To achieve FISMA-compliant configuration management, the IRS is in the process of implementing a number of tools to automate tasks, that when done manually, are extremely time-consuming and error-prone. However, we are concerned the IRS is not ensuring that it is avoiding tool redundancy and, therefore, excess cost or that it will be making the most efficient use of the data collections.

Tools or initiatives that the IRS already implemented or are in progress to improve its security posture include Business DNA (asset discovery), nCircle (vulnerability scanning), Security Compliance Posture Monitoring and Reporting (server configuration management), Treasury Enhanced Security Initiative (workstation configuration management), Altiris (Windows server patching), Guardium (database scanning), Knowledge Incident/Problem Service Asset Management (asset inventory), CiscoWorks (network management), Tivoli (older asset management tool), and a central repository for warehousing and integrating the collected data. The Cybersecurity organization has prepared an Information Technology Security Controls Tools Strategy for planning how all of this data will be organized and combined to provide near-real-time enterprise security intelligence for decision making.

As mentioned above, the Enterprise Services organization is also implementing a configuration and change management tool, called the ECMS. This solution is comprised of a number of commercial off-the-shelf products that include a configuration item discovery tool (the Discovery and Dependency Mapping Advanced tool), a central repository of configuration items and related components, change management analysis, and other tools for monitoring and maintaining configuration compliance. The Enterprise Services organization stated that until the ECMS is implemented, the IRS will continue to lack the capability to effectively implement configuration and change management.

We believe the IRS should ensure that data collected by its various tools and organizations will be efficiently utilized and that the IRS is not developing duplicative configuration management processes or products. For example, our discussions with the Cybersecurity and Enterprise Services organizations revealed that an approach for integrating the configuration management data collected by both organizations has not yet been formulated.

Identity and Access Management

Proper identity and access management ensures that users and devices are properly authorized to access information or information systems. Users and devices must be authenticated to ensure that they are who they identify themselves to be. In most systems, a user name and password serve as the primary means of authentication, while the system enforces authorized access rules established by the system administrator. To ensure that only authorized users and devices have access to a system, policy and procedures must be in place for the creation, distribution, maintenance, and eventual termination of accounts. The use of Personal Identity Verification (PIV) cards by all agencies, required by Homeland Security Presidential Directive-12 (HSPD-12),[11] is a major component of a secure, Government-wide account and identity management system.

The IRS has not fully implemented the following seven identity and access management attributes specified by the DHS metrics:

3.1.4. If multifactor authentication is in use, it is linked to the organization's PIV program, where appropriate.

3.1.5. Organization has adequately planned for implementation of PIV for logical access in accordance with government policies.

[11] On August 27, 2004, President Bush signed HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*. This directive established a new standard for issuing and maintaining identification badges for Federal employees and contractors entering Government facilities and accessing computer systems. The intent was to improve security, increase Government efficiency, reduce identity fraud, and protect personal privacy. Agencies are required to use PIV badges (also referred to as SmartID cards) to access computer systems (logical access).

3.1.6. Ensures that the users are granted access based on needs and separation of duties principles.

3.1.7. Identifies devices with Internet Protocol addresses that are attached to the network and distinguishes these devices from users.

3.1.8. Identifies all user and nonuser accounts (refers to user accounts that are on a system.)

3.1.9. Ensures that accounts are terminated or deactivated once access is no longer required.

3.1.10. Identifies and controls use of shared accounts.

3.1.4. If multifactor authentication is in use, it is linked to the organization's PIV program, where appropriate.

During the FY 2012 FISMA evaluation period, the TIGTA concluded fieldwork on an audit to evaluate the implementation and security of the IRS's two-factor authentication for logical (system) access.[12] The IRS has not deployed multifactor authentication via the use of an HSPD-12 PIV card for all users for network and local access to nonprivileged or privileged accounts as required by Federal mandate. Therefore, the IRS's multifactor authentication is not yet linked to its PIV program.

3.1.5. Organization has adequately planned for implementation of PIV for logical access in accordance with Government policies.

The IRS has experienced significant delays in deploying PIV cards for logical access, which reveals the IRS's inadequate planning efforts. The Federal Government mandated that agencies implement PIV cards to access computer systems in August 2004. The IRS originally planned to complete the deployment by September 2011. The deployment is now planned to be completed by July 2013, but various issues threaten further delays, including:

- The inability of the IRS to require its employees to use their PIV cards for logical access to the network because it did not negotiate mandatory use of the cards with the National Treasury Employees Union.
- Resolving PIV card deployment for system administrators, who currently require separate identities to perform administrator services on computer systems.
- The large number (1,888) of IRS applications that are not yet PIV card-enabled and the lack of resources to change these existing applications.

[12] TIGTA, Ref. No. 2012-20-115, *Using SmartID Cards to Access Computer Systems Is Taking Longer Than Expected* (Sept. 2012).

3.1.6. Ensures that the users are granted access based on needs and separation of duties principles.

Two of the three GSSs in our sample did not have the controls in place to ensure users are granted access based on needs or to enforce separation of duties. Applications residing on GSSs often rely on the GSS to implement these controls; therefore, the applications residing on these GSSs would also inherit these weaknesses.

The most recent security control assessment for one of the two GSSs that did not have these controls in place stated that accounts are not managed, enforced, separated, or deployed with least privilege in accordance with IRS policy requirements for all GSS components. Also, the most recent security control assessment for the other GSS found controls for granting access based on needs and for separation of duties were not implemented. For example, the operating system administrator could perform database administrator functions.

In addition, the GAO reported in March 2012[13] that IRS authorization controls were not always functioning as intended and access authorization policies were not effectively implemented. For example, systems used to process tax and financial information did not fully prevent access by unauthorized users or excessive levels of access for authorized users. In addition, the IRS's compliance checks revealed unauthorized access to another system. During its monthly compliance check in August 2011, the IRS identified 16 users who had been granted access to the procurement system without receiving approval from the IRS's authorization system. Also, the data in a shared work area used to support accounting operations were fully accessible by network administration staff although they did not need such access.

3.1.7. Identifies devices with Internet Protocol addresses that are attached to the network and distinguishes these devices from users.

The IRS informed us that Business DNA will be its enterprise asset discovery tool for identifying devices on its network. Business DNA network scans can identify devices with Internet Protocol addresses that are attached to the network and distinguish these devices from users. However, the full implementation of the Business DNA tool is not expected to be completed until September 2012. Therefore, the IRS has not yet fully implemented this attribute.

We also found that one of our three sample GSSs did not have device identification and authentication in place. It did not uniquely identify and authenticate devices or users before establishing a connection. Also, its firewalls did not use the Terminal Access Controller Access Control System[14] to authenticate organization users or devices. Rather, these firewalls were accessed via a shared administrator account.

---

[13] GAO, GAO-12-393, *IRS Needs to Further Enhance Internal Control Over Financial Reporting and Taxpayer Data* (Mar. 2012).

[14] An enterprise access control security system that provides device/network access authentication, authorization, and accounting.

3.1.8. Identifies all user and nonuser accounts.

No information was provided to determine how the IRS identifies all user and nonuser accounts.

3.1.9. Ensures that accounts are terminated or deactivated once access is no longer required.

Three of our 10 sample systems (two GSSs and one application) did not have controls in place to ensure accounts are terminated or deactivated once access is no longer needed. The most recent security control assessment for one GSS found:

- The system did not disable inactive accounts after 120 days of inactivity and did not employ automated mechanisms to audit account creation, modification, disabling, and termination actions.
- Evidence was not provided to ensure system accounts are reviewed at least annually.
- The system was not configured to notify appropriate individuals when accounts were modified.
- Evidence was not provided to ensure system accounts were reviewed at least annually and automated mechanisms were employed to support system account management functions.
- No automated mechanisms existed to support information system account management functions.
- Inactive accounts were not automatically disabled.

For the other GSS, the most recent security control assessment found:

- Accounts were not automatically disabled.
- The log files did not contain any evidence of logging the account creation, modification, disabling, and termination actions of a user account.

For the one application, its most recent security control assessment found that it did not disable accounts after 45 days or remove accounts after 90 days of inactivity.

Further, the GAO reported in March 2012[15] that the IRS had not taken actions to remove active application accounts in a timely manner for employees who had separated or no longer needed access.

[15] GAO, GAO-12-393, *IRS Needs to Further Enhance Internal Control Over Financial Reporting and Taxpayer Data* (Mar. 2012).

3.1.10. Identifies and controls use of shared accounts.

One of the GSSs in our sample was not adequately identifying and controlling use of shared accounts. The most recent security control assessment found that the administrative account for this GSS was shared. For example, the operating system administrator had the ability to "switch user" into Oracle using the "root" password. This login process is not uniquely linked to any one individual. Rather, this access is "shared" among the operating system administrators. Sharing this account in this manner allows fully privileged actions to be taken on the system without any accountability. In addition, passwords were stored and transmitted in plaintext.

Also, in June 2012, the TIGTA reported[16] that administrative accounts on Windows servers were not being properly safeguarded in accordance with IRS policy. Specifically, administrators in two IRS organizations were using the built-in system administrator accounts to perform normal administrative duties rather than only in emergencies as required by IRS policy. Seven administrators in one organization and 14 administrators in the other were sharing the password to the built-in accounts and were using these accounts for administrative tasks rather than using their unique role-based administrator accounts. Consequently, individual accountability was lost as to by whom and for what purposes these full-privileged accounts were being accessed.

Security Training

The FISMA requires all Government personnel and contractors to complete annual security awareness training that provides instruction on threats to data security and responsibilities for information protection. It also requires specialized training for personnel and contractors with significant security responsibilities. Without adequate security training programs, agencies cannot provide appropriate training or ensure that all personnel receive the required training.

The IRS had not fully implemented the following security training attribute specified by the DHS metrics: 6.1.5. Identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other organization users) with significant information security responsibilities that require specialized training.

6.1.5. Identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other organization users) with significant information security responsibilities that require specialized training.

The DHS provided clarification for this attribute as it relates to contractors, stating that agencies should be providing and tracking completion of specialized training for contractors just as they would for Federal employees. The specialized training requirement is based on the role of the contractor, not just on contractor status. Whoever holds a significant security role needs to receive specialized role-based training.

[16] TIGTA, Ref. No. 2012-20-063, *Enterprise-Level Oversight Is Needed to Ensure Adherence to Windows Server Security Policies* (June 2012).

The IRS has not fully implemented identification and tracking of the status of specialized role-based training for contractors. However, the IRS stated it is making plans to implement such tracking by October 15, 2012. The Contractor Security Management office in the Agency-Wide Shared Services organization is currently leading efforts to modify its contractor tracking system to allow the identification of those contractors with significant security responsibilities, with subsequent plans to implement a process to monitor and track completion of contractor specialized training. Once identified, the IRS would rely on the contractors to provide and self-report the completion of their required specialized training hours. Preliminary IRS results indicated that 919 such contractors were employed during the FISMA FY 2012 reporting period, with only 99 of those having confirmed that they completed the required training.

The IRS did not agree that it should provide specialized training for contractors and supported its position by citing the U.S. Office of Personnel Management's Training Policy Handbook, which states:

> *Since contractors are selected for their expertise in a subject area, contractors may only be trained in skills they are not required to bring to the job. Contractors may be trained in rules, practices, procedures, and/or systems that are unique to the employing agency and essential to the performance of the contractor's assigned duties, such as agency computer security procedures. However, the authority for training of contractors is not in training law. It is in the authority to administer contracts. Training of contractors is subject to the decision of the chief contracting official.*

The IRS stated that to require it to provide, track, and report specialized training completions for contractors would present significant challenges, including requiring thousands of contract language modifications before it could enforce this requirement for contract employees.

Appendix I

Fiscal Year 2012 Reporting Metrics

Presented below is the list of reporting metrics questions and information as detailed in the *Fiscal Year 2012 Inspector General Federal Information Security Management Act (FISMA) Reporting Metrics.*[1] The list is presented in its entirety, along with the accompanying Purpose and Use information. Following each metric is a notation identifying each individual question as an Administration Priority (AP), a Key FISMA Metric (KFM), or a Baseline Question (Base). Many abbreviations in this list are used as presented in the original document and are not defined therein. However, we have provided the definitions in the Abbreviations page after the Table of Contents of this report.

1. CONTINUOUS MONITORING MANAGEMENT

1.1. Has the organization established an enterprise-wide continuous monitoring program that assesses the security state of information systems that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

1.1.1. Documented policies and procedures for continuous monitoring (NIST 800-53: CA-7). (AP)

1.1.2. Documented strategy and plans for continuous monitoring (NIST 800-37 Rev. 1, Appendix G). (AP)

1.1.3. Ongoing assessments of security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans (NIST 800-53, NIST 800-53A). (AP)

1.1.4. Provides authorizing officials and other key system officials with security status reports covering updates to security plans and security assessment reports as well as POA&M additions and updates, with the frequency defined in the strategy and/or plans (NIST 800-53, NIST 800-53A). (AP)

[1] U.S. Department of Homeland Security, National Cyber Security Division, *Fiscal Year 2012 Inspector General Federal Information Security Management Act Reporting Metrics*, pp. 6–17 (Mar. 2012). The FISMA is encoded in Title III of the E-Government Act of 2002; Pub. L. No. 107-374, 116 Stat. 2899.

1.2. Please provide any additional information on the effectiveness of the organization's continuous monitoring management program that was not noted in the questions above.

Purpose and Use

These questions are being asked for the following reasons:

- The Federal Continuous Monitoring Working Group (CMWG) has determined that continuous monitoring (CM) of configurations is one of the first areas where CM capabilities need to be developed. This applies to both operating systems and widely used applications.
- Even with a completely hardened system, exploitation may still occur due to zero-day vulnerabilities. However, this forces attackers to elevate their sophistication for successful attacks.
- Rather, a robust continuous monitoring solution will be able to provide additional visibility for organizations to identify signs of compromise, though no single indicator may identify a definitive incident.

2. CONFIGURATION MANAGEMENT

2.1. Has the organization established a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

2.1.1. Documented policies and procedures for configuration management. (Base)

2.1.2. Standard baseline configurations defined. (Base)

2.1.3. Assessing for compliance with baseline configurations. (Base)

2.1.4. Process for timely, as specified in organization policy or standards, remediation of scan result deviations. (Base)

2.1.5. For Windows-based components, FDCC/USGCB secure configuration settings fully implemented and any deviations from FDCC/USGCB baseline settings fully documented. (Base)

2.1.6. Documented proposed or actual changes to hardware and software configurations. (Base)

2.1.7. Process for timely and secure installation of software patches. (Base)

2.1.8. Software assessing (scanning) capabilities are fully implemented (NIST 800-53: RA-5, SI-2). (Base)

2.1.9. Configuration-related vulnerabilities, including scan findings, have been remediated in a timely manner, as specified in organization policy or standards. (NIST 800-53: CM-4, CM-6, RA-5, SI-2). (Base)

2.1.10. Patch management process is fully developed, as specified in organization policy or standards. (NIST 800-53: CM-3, SI-2). (Base)

2.2. Please provide any additional information on the effectiveness of the organization's configuration management program that was not noted in the questions above.

Purpose and Use

These questions are being asked for the following reasons:

- A key goal of configuration management is to make assets harder to exploit through better configuration.
- A key assumption is that configuration management covers the universe of assets to which other controls need to be applied (controls that are defined under asset management).
- To have a capable configuration management program, the configuration management capability needs to be:
  - Relatively complete, covering enough of the software base to significantly increase the effort required for a successful attack.
  - Relatively timely, being able to find and fix configuration deviations faster than they can be exploited.

3. IDENTITY AND ACCESS MANAGEMENT

3.1. Has the organization established an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and identifies users and network devices? If yes, besides the improvement opportunities that have been identified by the OIG, does the program include the following attributes:

3.1.1. Documented policies and procedures for account and identity management (NIST 800-53: AC-1). (Base)

3.1.2. Identifies all users, including Federal employees, contractors, and others who access organization systems (NIST 800-53, AC-2). (Base)

3.1.3. Identifies when special access requirements (*e.g.*, multifactor authentication) are necessary. (Base)

3.1.4. If multifactor authentication is in use, it is linked to the organization's PIV program, where appropriate (NIST 800-53, IA-2). (KFM)

3.1.5. Organization has adequately planned for implementation of PIV for logical access in accordance with Government policies (HSPD-12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11). (AP)

3.1.6. Ensures that the users are granted access based on needs and separation of duties principles. (Base)

3.1.7. Identifies devices with IP addresses that are attached to the network and distinguishes these devices from users. (For example: IP phones, faxes, and printers are examples of devices attached to the network that are distinguishable from desktops, laptops, or servers that have user accounts.) (Base)

3.1.8. Identifies all user and nonuser accounts (refers to user accounts that are on a system. Examples of nonuser accounts are accounts such as an IP that is set up for printing. Data user accounts are created to pull generic information from a database or a guest/anonymous account for generic login purposes that are not associated with a single user or a specific group of users.) (Base)

3.1.9. Ensures that accounts are terminated or deactivated once access is no longer required. (Base)

3.1.10. Identifies and controls use of shared accounts. (Base)

3.2. Please provide any additional information on the effectiveness of the organization's identity and access management program that was not noted in the questions above.

Purpose and Use

These questions are being asked for the following reasons:

- OMB and DHS have determined that Federal identity management (HSPD-12) is among the areas where additional controls need to be developed. See also OMB M-04-04 for web-based systems.
- Strong information system authentication requires multiple factors to securely authenticate a user. Secure authentication requires something you have, something you are, and something you know. A single-factor authentication mechanism, such as a username and password, is insufficient to block even basic attackers.
- The USG will first move to a two-factor authentication using PIV cards, though a stronger authentication solution would include all three factors.
- Enhanced identity management solutions also support the adoption of additional nonsecurity benefits, such as single sign-on, more useable systems, and enhanced identity capabilities for legal and nonrepudiation needs.

- A key goal of identity and access management is to make sure that access rights are only given to the intended individuals and/or processes.[2]
- To have a capable identity management program, this capability needs to be:
  - Relatively complete, covering all accounts.
  - Relatively timely, being able to find and remove stale or compromised accounts faster than they can be exploited.

4. INCIDENT RESPONSE AND REPORTING

4.1. Has the organization established an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

4.1.1. Documented policies and procedures for detecting, responding to, and reporting incidents (NIST 800-53: IR-1). (Base)

4.1.2. Comprehensive analysis, validation, and documentation of incidents. (KFM)

4.1.3. When applicable, reports to US-CERT within established time frames (NIST 800-53, 800-61, and OMB M-07-16, M-06-19). (KFM)

4.1.4. When applicable, reports to law enforcement within established time frames (SP 800-86). (KFM)

4.1.5. Responds to and resolves incidents in a timely manner, as specified in organization policy or standards, to minimize further damage (NIST 800-53, 800-61, and OMB M-07-16, M-06-19). (KFM)

4.1.6. Is capable of tracking and managing risks in a virtual/cloud environment, if applicable. (Base)

4.1.7. Is capable of correlating incidents. (Base)

4.1.8. There is sufficient incident monitoring and detection coverage in accordance with Government policies (NIST 800-53, 800-61, and OMB M-07-16, M-06-19). (Base)

4.2. Please provide any additional information on the effectiveness of the organization's incident management program that was not noted in the questions above.

[2] This is done, of course, by establishing a process to assign attributes to a digital identity and by connecting an individual to that identity. However, this would be pointless without subsequently using it to control access.

Purpose and Use

These questions are being asked for the following reasons:

- Given real world realities, it is reasonable to expect that some attacks will succeed. Organizations need to be able to detect those attacks. Ideally, organizations would defend against those attacks in real time; but at a minimum, organizations are expected to determine the kinds of attacks that are most successful.
- This allows the organization to use this information about successful attacks and their impact to make informed risk-based decisions about where it is most cost effective and essential to focus security resources.

5. RISK MANAGEMENT

5.1. Has the organization established a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

5.1.1. Documented and centrally accessible policies and procedures for risk management, including descriptions of the roles and responsibilities of participants in this process. (Base)

5.1.2. Addresses risk from an organization perspective with the development of a comprehensive governance structure and organization-wide risk management strategy as described in NIST 800-37, Rev. 1. (Base)

5.1.3. Addresses risk from a mission and business process perspective and is guided by the risk decisions at the organizational perspective, as described in NIST 800-37, Rev. 1. (Base)

5.1.4. Addresses risk from an information system perspective and is guided by the risk decisions at the organizational perspective and the mission and business perspective, as described in NIST 800-37, Rev. 1. (Base)

5.1.5. Categorizes information systems in accordance with Government policies. (Base)

5.1.6. Selects an appropriately tailored set of baseline security controls. (Base)

5.1.7. Implements the tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation. (Base)

5.1.8. Assesses the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly,

operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. (Base)

5.1.9. Authorizes information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable. (Base)

5.1.10. Ensures information security controls are monitored on an ongoing basis, including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials. (Base)

5.1.11. Information system specific risks (tactical), mission/business specific risks, and organizational level (strategic) risks are communicated to appropriate levels of the organization. (Base)

5.1.12. Senior officials are briefed on threat activity on a regular basis by appropriate personnel (*e.g.*, CISO). (Base)

5.1.13. Prescribes the active involvement of information system owners and common control providers, Chief Information Officers, senior information security officers, authorizing officials, and other roles as applicable in the ongoing management of information system-related security risks. (Base)

5.1.14. Security authorization package contains system security plan, security assessment report, and POA&M in accordance with Government policies (NIST SP 800-18, SP 800-37). (Base)

5.1.15. Security authorization package contains accreditation boundaries for organization information systems defined in accordance with Government policies. (Base)

5.2. Please provide any additional information on the effectiveness of the organization's risk management program that was not noted in the questions above.

Purpose and Use:

These questions are being asked for the following reasons:

- One goal in issuing these FISMA questions is to further empower OIGs to focus on how agencies are evaluating risk and prioritizing security issues.
- OIGs are encouraged to use a type of risk analysis as specified in NIST 800-39 to evaluate findings and compare those to (1) existing organization priorities and (2) Administration

priorities and key FISMA metrics identified in the CIO metrics to determine areas of weakness and highlight the significance of security issues.

6. SECURITY TRAINING

6.1. Has the organization established a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

6.1.1. Documented policies and procedures for security awareness training (NIST 800-53: AT-1). (Base)

6.1.2. Documented policies and procedures for specialized training for users with significant information security responsibilities. (Base)

6.1.3. Security training content based on the organization and roles, as specified in organization policy or standards. (Base)

6.1.4. Identification and tracking of the status of security awareness training for all personnel (including employees, contractors, and other organization users) with access privileges that require security awareness training. (KFM)

6.1.5. Identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other organization users) with significant information security responsibilities that require specialized training. (KFM)

6.1.6. Training material for security awareness training does not contain appropriate content for the organization (NIST SP 800-50, SP 800-53). (Base)

6.2. Please provide any additional information on the effectiveness of the organization's security training program that was not noted in the questions above.

Purpose and Use

These questions are being asked for the following reasons:

- Some of the most effective attacks on cyber-networks world-wide currently are directed at exploiting user behavior. These include phishing attacks, social engineering to obtain passwords, and introduction of malware via removable media.
- These threats are especially effective when directed at those with elevated network privileges and/or other elevated cyber responsibilities.
- DHS has determined that some metrics in this section are prioritized as Key FISMA Metrics.
- Some questions in this section also contain baseline information to be used to assess future improvement in performance.

- The metrics will be used to assess the extent to which organizations are providing adequate training to address these attacks and threats.

7. PLAN OF ACTION & MILESTONES (POA&M)

7.1. Has the organization established a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and tracks and monitors known information security weaknesses? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

7.1.1. Documented policies and procedures for managing IT security weaknesses discovered during security control assessments and requiring remediation. (Base)

7.1.2. Tracks, prioritizes, and remediates weaknesses. (Base)

7.1.3. Ensures remediation plans are effective for correcting weaknesses. (Base)

7.1.4. Establishes and adheres to milestone remediation dates. (Base)

7.1.5. Ensures resources are provided for correcting weaknesses. (Base)

7.1.6. POA&Ms include security weaknesses discovered during assessments of security controls and requiring remediation. (Do not need to include security weakness due to a risk-based decision to not implement a security control) (OMB M-04-25). (Base)

7.1.7. Costs associated with remediating weaknesses are identified (NIST SP 800-53, Rev. 3, Control PM-3 and OMB M-04-25). (Base)

7.1.8. Program officials and contractors report progress on remediation to CIO on a regular basis, at least quarterly, and the CIO centrally tracks, maintains, and independently reviews/validates the POA&M activities at least quarterly (NIST SP 800-53, Rev. 3, Control CA-5, and OMB M-04-25). (Base)

7.2. Please provide any additional information on the effectiveness of the organization's POA&M program that was not noted in the questions above.

Purpose and Use

These questions are being asked for the following reasons:

- POA&M processes are important as part of the risk management process to track problems and to decide which ones to address.

8. REMOTE ACCESS MANAGEMENT

8.1. Has the organization established a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

8.1.1. Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access (NIST 800-53: AC-1, AC-17). (Base)

8.1.2. Protects against unauthorized connections or subversion of authorized connections. (Base)

8.1.3. Users are uniquely identified and authenticated for all access (NIST 800-46, Section 4.2, Section 5.1). (Base)

8.1.4. Telecommuting policy is fully developed (NIST 800-46, Section 5.1). (Base)

8.1.5. If applicable, multifactor authentication is required for remote access (NIST 800-46, Section 2.2, Section 3.3). (KFM)

8.1.6. Authentication mechanisms meet NIST Special Publication 800-63 guidance on remote electronic authentication, including strength mechanisms. (Base)

8.1.7. Defines and implements encryption requirements for information transmitted across public networks. (KFM)

8.1.8. Remote access sessions, in accordance to OMB M-07-16, are timed out after 30 minutes of inactivity, after which reauthentication is required. (Base)

8.1.9. Lost or stolen devices are disabled and appropriately reported (NIST 800-46, Section 4.3, US-CERT Incident Reporting Guidelines). (Base)

8.1.10. Remote access rules of behavior are adequate in accordance with Government policies (NIST 800-53, PL-4). (Base)

8.1.11. Remote access user agreements are adequate in accordance with Government policies (NIST 800-46, Section 5.1, NIST 800-53, PS-6). (Base)

8.2. Please provide any additional information on the effectiveness of the organization's remote access management that was not noted in the questions above.

Purpose and Use

These questions are being asked for the following reasons:

- Adequate control of remote connections is a critical part of boundary protection.

- Attackers exploit boundary systems on Internet-accessible DMZ networks (and on internal network boundaries) and then pivot to gain deeper access on internal networks. Responses to the above questions will help agencies deter, detect, and defend against unauthorized network connections/access to internal and external networks.
- Remote connections allow users to access the network without gaining physical access to organization space and the computers hosted there. Moreover, the connections over the Internet provide opportunities for compromise of information in transit. Because these connections are beyond physical security controls, they need compensating controls to ensure that only properly identified and authenticated users gain access and that the connections prevent hijacking by others.

9. CONTINGENCY PLANNING

9.1. Has the organization established an enterprise-wide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

9.1.1. Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster (NIST 800-53: CP-1). (Base)

9.1.2. The organization has performed an overall Business Impact Analysis (BIA) (NIST SP 800-34). (Base)

9.1.3. Development and documentation of division, component, and IT infrastructure recovery strategies, plans, and procedures (NIST SP 800-34). (Base)

9.1.4. Testing of system-specific contingency plans. (Base)

9.1.5. The documented business continuity and disaster recovery plans are in place and can be implemented when necessary (FCD1, NIST SP 800-34). (Base)

9.1.6. Development and fully implementable of test, training, and exercise (TT&E) programs (FCD1, NIST SP 800-34, NIST 800-53). (Base)

9.1.7. Performance of regular ongoing testing or exercising of business continuity/ disaster recovery plans to determine effectiveness and to maintain current plans. (Base)

9.1.8. After-action report that addresses issues identified during contingency/disaster recovery exercises (FCD1, NIST SP 800-34). (Base)

9.1.9. Systems that have alternate processing sites (FCD1, NIST SP 800-34, NIST SP 800-53). (Base)

9.1.10. Alternate processing sites are subject to the same risks as primary sites (FCD1, NIST SP 800-34, NIST SP 800-53).

9.1.11. Backups of information that are performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53). (Base)

9.1.12. Contingency planning that considers supply chain threats. (Base)

9.2. Please provide any additional information on the effectiveness of the organization's contingency planning program that was not noted in the questions above.

Purpose and Use

These questions are being asked for the following reasons:

- Contingency planning deals with risks which occur rarely. As such, there is a temptation to ignore these risks.
- The purpose of this section is to determine if the organization is giving adequate attention to the rare events which have such significant consequences that they become first-priority risks.

10. CONTRACTOR SYSTEMS

10.1. Has the organization established a program to oversee systems operated on its behalf by contractors or other entities, including organization systems and services residing in the cloud external to the organization? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program includes the following attributes:

10.1.1. Documented policies and procedures for information security oversight of systems operated on the organization's behalf by contractors or other entities, including organization systems and services residing in public cloud. (Base)

10.1.2. The organization obtains sufficient assurance that security controls of such systems and services are effectively implemented and comply with Federal and organization guidelines. (Base)

10.1.3. A complete inventory of systems operated on the organization's behalf by contractors or other entities, including organization systems and services residing in public cloud. (Base)

10.1.4. The inventory identifies interfaces between these systems and organization-operated systems (NIST 800-53: PM-5). (Base)

10.1.5. The organization requires appropriate agreements (*e.g.*, MOUs, Interconnection Security Agreements, contracts, *etc.*) for interfaces between these systems and those that it owns and operates. (Base)

10.1.6. The inventory of contractor systems is updated at least annually. (Base)

10.1.7. Systems that are owned or operated by contractors or entities, including organization systems and services residing in public cloud, are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines. (Base)

10.2. Please provide any additional information on the effectiveness of the organization's contractor systems program that was not noted in the questions above.

Purpose and Use

These questions are being asked for the following reasons:

- These questions are being asked because in the past some Federal agencies tended to assume that they were not responsible for managing the risk of contractor systems.
- The key question is "Are these contractor-operated systems being managed to ensure that they have adequate security and can the DAA make an informed decision about whether or not to accept any residual risk?"

11. SECURITY CAPITAL PLANNING

11.1. Has the organization established a security capital planning and investment program for information security? If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

11.1.1. Documented policies and procedures to address information security in the capital planning and investment control (CPIC) process. (Base)

11.1.2. Includes information security requirements as part of the capital planning and investment process. (Base)

11.1.3. Establishes a discrete line item for information security in organizational programming and documentation (NIST 800-53: SA-2). (Base)

11.1.4. Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required (NIST 800-53: PM-3). (Base)

11.1.5. Ensures that information security resources are available for expenditure as planned. (Base)

11.2. Please provide any additional information on the effectiveness of the organization's security capital planning program that was not noted in the questions above.

Purpose and Use

These questions are being asked for the following reasons:

- One key area of capital investment in the next few years will be investments in the tools and other infrastructure needed for adequate continuous monitoring. Fortunately, most of these tools also support (and are needed for) good network and system operations. Thus, many of these tools may already be in place.
- This section might equally consider operational budgeting. Clearly, good security requires a wise investment of operational resources, not just capital ones.

Appendix II

Major Contributors to This Report

Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Director
Jody Kitazono, Audit Manager
Bret Hunter, Senior Auditor
Mary Jankowski, Senior Auditor
Louis Lee, Senior Auditor
Midori Ohno, Senior Auditor
Esther Wilson, Senior Auditor
Linda Nethery, Information Technology Specialist

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Chief Technology Officer OS:CTO
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 Control OS:CFO:CPIC:IC
Audit Liaison: Director, Risk Management Division OS:CTO:SP:RM

Appendix IV

Treasury Inspector General for Tax Administration Information Technology Security-Related Reports Issued During the Fiscal Year 2012 Evaluation Period

1. Treasury Inspector General for Tax Administration (TIGTA), Ref. No. 2011-20-076, *The IRS2GO Smartphone Application Is Secure, but Development Process Improvements Are Needed* (Aug. 2011).
2. TIGTA, Ref. No. 2011-20-088, *The Modernized e-File Release 6.2 Included Enhancements, but Improvements Are Needed for Tracking Performance Issues and Security Weaknesses* (Sept. 2011).
3. TIGTA, Ref. No. 2011-20-116, *Treasury Inspector General for Tax Administration – Federal Information Security Management Act Report for Fiscal Year 2011* (Sept. 2011).
4. TIGTA, Ref. No. 2011-20-111, *Continued Centralization of the Windows Environment Would Improve Administration and Security Efficiencies* (Sept. 2011).
5. TIGTA, Ref. No. 2011-20-101, *Security Controls Over Wireless Technology Were Generally in Place; However, Further Actions Can Improve Security* (Sept. 2011).
6. TIGTA, Ref. No. 2011-20-099, *The Mainframe Databases Reviewed Met Security Requirements; However, Automated Security Scans Were Not Performed* (Sept. 2011).
7. TIGTA, Ref. No. 2012-20-019, *The Computer Security Incident Response Center Is Effectively Performing Most of Its Responsibilities, but Further Improvements Are Needed* (Mar. 2012).
8. TIGTA, Ref. No. 2012-20-041, *Disaster Recovery Testing Is Being Adequately Performed, but Problem Reporting and Tracking Can Be Improved* (May 2012).
9. TIGTA, Ref. No. 2012-20-063, *Enterprise-Level Oversight Is Needed to Ensure Adherence to Windows Server Security Policies* (June 2012).

Appendix V

Glossary of Terms

Term	Definition
Accreditation (or Authorization) Boundary	Includes all components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems to which the information system is connected.
Administrative Account	A user account with full privileges on a computer.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Boundary Protection	Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communication through the use of boundary protection devices.
Boundary System	Physical or logical perimeter of a system.
Cloud (Computing) Environment	The use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams.
Configuration Baseline	A set of specifications for a system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and that can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes.
Configuration Items	Assets, service components, or other items that are (or will be) controlled by configuration management.

Term	Definition
Configuration Management	A collection of activities focused on establishing and maintaining the integrity of products and systems through control of the processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.
Demilitarized Zone	A network segment inserted as a "neutral zone" between an organization's private network and the Internet.
Device Identification and Authentication	The information system uniquely identifies and authenticates before establishing a connection. See Authentication.
Federal Desktop Core Configuration	OMB-mandated set of security configurations for all Federal workstation and laptop devices that run either Windows XP or Vista.
Firewall	A gateway that limits access between networks in accordance with local security policy.
General Support System	An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.
Identity and Access Management	Addresses the mission-critical need to ensure appropriate access to resources across increasingly heterogeneous technology environments and to meet increasingly rigorous compliance requirements.
Internal Revenue Manual	The IRS publication of its information security policies, guidelines, standards, and procedures in order for IRS divisions and offices to carry out their respective responsibilities in information security.
Internet Protocol	Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks.
Least Privilege	The security objective of granting users only those accesses they need to perform their official duties.

Term	Definition
Logical Access	Controls used to determine the electronic information and systems that users and other systems may access and the actions that may be performed to the information accessed.
Malware	A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the computer's data, applications, or operating system.
Milestone	The "go/no-go" decision point in a project; it is sometimes associated with funding approval to proceed.
Multifactor Authentication	Authentication using two or more factors to achieve authentication. Factors include: (1) something you know (*e.g.*, password/PIN); (2) something you have (*e.g.*, cryptographic identification device, token); or (3) something you are (*e.g.*, physical characteristic).
nCircle	An automated tool that scans computers for vulnerabilities related to network exploits and renders a report of findings.
Operating System	A set of software that manages computer hardware resources and provides common services for computer programs. The operating system is a vital component of the system software in a computer system. Application programs require an operating system to function.
Patch Management	The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs.
Phishing (Attack)	Tricking individuals into disclosing sensitive personal information through deceptive computer-based means.
Plaintext	Intelligible data that has meaning and can be understood without the application of decryption.
Plan of Action and Milestones	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

Term	Definition
Policy Checker	An automated tool that reads the security settings of computers and logs any noncompliant setting to text files.
Privileged Account	Individuals who have access to set "access rights" for users on a given system. Sometimes referred to as system or network administrative accounts.
Remote Access	Access to an organizational information system by a user (or an information system acting on behalf of a user) communicating through an external network (*e.g.*, the Internet).
Rogue Computer	An unauthorized computer on a network.
Security Capital Planning	The integration of information technology security and capital planning processes to ensure that agency resources are protected and risk is effectively managed.
Separation of Duties	As a security principle, its primary objective is the prevention of fraud and errors. This objective is achieved by disseminating the tasks and associated privileges for a specific business process among multiple users.
Single-factor Authentication	Authentication using one factor (*e.g.*, a username or password) to achieve authentication. See Authentication.
Single Sign-On	Provides the capability to authenticate once and be subsequently and automatically authenticated when accessing various target systems. It eliminates the need to separately authenticate and sign on to individual applications and systems, essentially serving as a user surrogate between client workstations and target systems.
Social Engineering	An attempt to trick someone into revealing information (*e.g.*, a password) that can be used to attack systems or networks.
Two-factor Authentication	Authentication using two factors to achieve authentication. See Multifactor Authentication.
US-CERT	A partnership between the Department of Homeland Security and the public and private sectors established to protect the Nation's Internet infrastructure. US-CERT coordinates defense against and responses to cyberattacks across the Nation.

Term	Definition
Virtual Environment	The physical system running a host operating system and hypervisor (*i.e.*, software that allows a single host to run one or more guest operating systems).
Vulnerability Scanning (*i.e.*, Software Assessing)	Scanning for specific functions, ports, protocols, and services that should not be accessible to users or devices and for improperly configured or incorrectly operating information flow mechanisms.
Zero-Day Vulnerability	An exploit that takes advantage of a security vulnerability on the same day that the vulnerability becomes generally known. There are zero days between the time the vulnerability is discovered and the first attack. Given time, the software company can fix the code and distribute a patch or software update.