TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

The Internal Revenue Service Should Implement an Efficient Internal Information Security Continuous Monitoring Program That Meets Its Security Needs

September 17, 2014

Reference Number: 2014-20-083

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.treasury.gov/tigta

THE INTERNAL REVENUE SERVICE SHOULD IMPLEMENT AN EFFICIENT INTERNAL INFORMATION SECURITY CONTINUOUS MONITORING PROGRAM THAT MEETS ITS SECURITY NEEDS

Highlights

Final Report issued on September 17, 2014

Highlights of Reference Number: 2014-20-083 to the Internal Revenue Service Chief Technology Officer.

IMPACT ON TAXPAYERS

The IRS is in the process of implementing an Information Security Continuous Monitoring (ISCM) program. When fully implemented, the program will allow the IRS to continuously monitor security controls of its computer assets in real time, thus improving the effectiveness of the safeguards and countermeasures to protect taxpayer information and information systems.

WHY TIGTA DID THE AUDIT

This audit was initiated as part of our Fiscal Year 2014 Annual Audit Plan and addresses the major management challenge of Security for Taxpayer Data and Employees. The overall objective of this review was to assess the current state of Continuous Diagnostics and Mitigation (CDM) program controls in place at the IRS.

WHAT TIGTA FOUND

Although implementation of the ISCM program has been slow across the Federal Government, the IRS has been in compliance with Department of Homeland Security and Department of the Treasury guidelines.

In addition to the mandatory guidelines imposed by the Office of Management and Budget, Treasury Department officials have also mandated that their bureaus use only the Treasury Department's dashboard that will serve as the official reporting for the ISCM program and use those security tools selected by Treasury Department officials for consistency.

Although the Treasury Department's intentions for consistency and efficiency are workable for most of its offices and bureaus, TIGTA found that, based on the large scale of the IRS's computer environment, a one-size-fits-all approach does not provide the best security for the IRS. TIGTA also identified inefficiencies the IRS will experience if it selects the recommended Treasury Department tool.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the IRS Chief Technology Officer continue to move forward and coordinate, as appropriate, with the Treasury Department to implement a stronger internal ISCM program that allows executives to make the most informed decisions that affect the security of the IRS network. This includes: 1) selecting and implementing an internal dashboard, 2) taking advantage of the General Services Administration's Blanket Purchase Agreement through the Department of Homeland Security's CDM program to acquire products to ensure that gaps in coverage and tool enhancements of the ISCM program are adequately addressed and best suited for the IRS environment, and 3) ensuring that tools selected for use (such as the database scanning tool) are the most effective and make the most efficient use of IRS resources.

IRS officials agreed with our recommendations and plan to continue coordinating with Treasury to ensure that the IRS selects the most effective and efficient security tools that meet the unique needs of the IRS computing environment. The IRS also plans to take advantage of the General Services Administration's Blanket Purchase Agreement to acquire products best suited for the IRS's environment.

The IRS also plans to establish an enterprise-wide ISCM integrated project team to direct the selection and implementation of an integrated dashboard of the security scanning tools to ensure that stakeholders and decision makers are well-informed to make risk-based decisions and to pursue tool enhancements for current tools and tool selections for gaps to ensure that the most cost-efficient method is used to the extent that funding is available.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

September 17, 2014

MEMORANDUM FOR CHIEF TECHNOLOGY OFFICER

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The Internal Revenue Service Should Implement an Efficient Internal Information Security Continuous Monitoring Program That Meets Its Security Needs (Audit # 201320003)

This report presents the results of our review to assess the current state of Continuous Diagnostics and Mitigation program controls in place at the Internal Revenue Service (IRS). This audit is included in the Treasury Inspector General for Tax Administration's Fiscal Year 2014 Annual Audit Plan and addresses the major management challenge of Security for Taxpayer Data and Employees.

Management's complete response to the draft report is included as Appendix VI.

Copies of this report are also being sent to the IRS managers affected by the report recommendations. If you have any questions, please contact me or Kent Sagara, Acting Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Abbreviations

BPA	Blanket Purchase Agreement
CDM	Continuous Diagnostics and Mitigation
CONOPS	Concept of Operations
DHS	Department of Homeland Security
eGRC	Enterprise Governance Risk and Compliance
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GSA	General Services Administration
IRS	Internal Revenue Service
ISCM	Information Security Continuous Monitoring
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
TIGTA	Treasury Inspector General for Tax Administration

Background

The need to know its current security posture at any given point in time is vital for any organization. To strengthen the Nation's cybersecurity posture, the Administration and the Office of Management and Budget (OMB) identified cybersecurity as one of 14 Cross-Agency Priority Goals, which included continuous monitoring of all Federal information systems.

Information security continuous monitoring (ISCM) is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

During Calendar Year 2013, the Federal Government has taken actions to support and accelerate agency implementation of effective risk management programs. In coordination with the OMB, the Federal Chief Information Officer's Council and the Committee on National Security Systems established the Joint Continuous Monitoring Working Group, which developed the U.S. Government Concept of Operations (CONOPS) for ISCM. This CONOPS supplements National Institute of Standards and Technology (NIST) guidelines by providing a roadmap and more specific implementation guidance to stakeholders across the Federal Government.

The ISCM is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. The requirement to manage information security risk on a continuous basis includes the requirement to monitor the security controls in Federal information systems and the environments in which those systems operate on an ongoing, real-time basis. Figure 1 presents the ISCM security automation domains, as defined by the NIST.

Figure 1: Security Automation Domains

Source: NIST Special Publication 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations.

Appendix IV presents a brief explanation of each security automation domain. To fully implement the ISCM across the Government, the OMB has instructed agencies to develop and maintain an ISCM strategy and establish an ISCM program consistent with existing statutes, OMB policy, NIST guidelines, and the CONOPS. To assist with this effort from a Governmentwide perspective, the Department of Homeland Security (DHS) has established a Continuous Diagnostics and Mitigation (CDM) program.

Agencies shall implement continuous monitoring of security controls as part of a phased approach through Fiscal Year (FY) 2017. In accordance with the CONOPS, Phase 1 of the DHS CDM program, which included the Federal dashboard,[1] requires automating the following subsets of information security capabilities:

- Hardware Asset Management (part of Asset Management).
- Software Asset Management (part of Asset Management).
- Configuration Management.
- Vulnerability Management.

[1] In management information systems, a **dashboard** is an easy to read, often single page, real-time user interface, showing a graphical presentation of the current status (snapshot) and historical trends of an organization's key performance indicators to enable instantaneous and informed decisions to be made at a glance.

Under this program, the DHS coordinated with the General Services Administration (GSA) to establish a Governmentwide Blanket Purchase Agreement (BPA) under Multiple Award Schedule 70, which Federal, State, local, and tribal governments can leverage to deploy a basic set of capabilities to support continuous monitoring of security controls in Federal information systems and environments of operation. The BPA, awarded on August 12, 2013, provides a consistent, Governmentwide set of ISCM program tools to enhance the Federal Government's ability to identify and respond, in real time or near real time, to the risk of emerging cyberthreats. It also capitalizes on strategic sourcing to minimize the costs associated with implementing requirements of the Risk Management Framework.[2]

The Internal Revenue Service's (IRS) ISCM program is managed by the Information Technology organization's Cybersecurity office. In addition to the Cybersecurity office, program implementation is supported by the Information Technology organization's Enterprise Operations, User Network Services, and Enterprise Services offices for Phase 1 of the ISCM program.

This review was performed with information obtained from the IRS's Information Technology organization, including the offices of Cybersecurity, Enterprise Operations, Enterprise Services, and User Network Services, in New Carrollton, Maryland, during the period November 2013 through May 2014. 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.

[2] The Risk Management Framework provides a disciplined and structured process that integrates information security and risk management activities into the systems development life cycle. The Risk Management Framework steps include: categorize, select, implement, assess, authorize, and monitor.

Results of Review

The Internal Revenue Service Should Continue to Move Forward in Implementing a Stronger Information Security Continuous Monitoring Program

The OMB issued Memorandum 10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS)*, which defines DHS activities within the Federal Government. DHS activities will include (but will not be limited to):

- Overseeing the Governmentwide and agency-specific implementation of and reporting on cybersecurity policies and guidance.
- Overseeing and assisting Governmentwide and agency-specific efforts to provide adequate, risk-based, and cost-effective cybersecurity.
- Overseeing the agencies' compliance with the Federal Information Security Management Act (FISMA)[3] and developing analyses for the OMB to assist in the development of the FISMA annual report.
- Overseeing the agencies' cybersecurity operations and incident response and providing appropriate assistance.
- Annually reviewing the agencies' cybersecurity programs.

All departments and agencies are required to coordinate and cooperate with the DHS as they carry out their cybersecurity responsibilities. The DHS is currently coordinating Federal Government efforts to roll out agencies' ISCM programs and is using its CDM program as a means for agencies to purchase tools needed for their ISCM programs.

Although the IRS is complying with initial DHS and Department of the Treasury requests, which have satisfied some of the OMB deadlines to date, the Federal Government process to acquire vendor tools and dashboards has taken longer than expected. The DHS has scheduled meetings among agencies, vendors, and bidders into FY 2015. As a result, Treasury Department officials do not expect to meet any additional OMB deadlines that were issued in November 2013 on the rollout and implementation of the first three security automation domains of the ISCM program. Appendix V presents the OMB ISCM program deadlines and the status of required actions by the IRS.

[3] Federal Information Security Management Act of 2002 ("FISMA", 44 U.S.C. § 3541, et seq.) is a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002 (Pub. L. 107–347, 116 Stat. 2899).

The IRS has made progress implementing its ISCM program

Progress has been made in implementing the IRS's ISCM program, although the progress is still in the early stages of development. For example, in September 2013, the IRS released an ISCM Strategy document that defines and develops an IRS-specific ISCM strategy to be used to establish and implement an ISCM program. This strategy discusses the key IRS roles, the officials who have a major part in the program, and the requirements and activities at each organizational tier. Currently, the IRS is working on an ISCM plan that better defines the current initiatives and establishes a clear vision for the future state of the IRS's ISCM program. The IRS stated that going forward, the ISCM plan will be a living document continually addressing and monitoring the IRS's information technology environment.

OMB Memorandum 14-03, *Enhancing the Security of Federal Information and Information Systems*, and the CONOPS both have issued deadlines and milestones for agencies to implement Phase 1 by FY 2014. However, because the Federal Government rollout is behind schedule, the IRS and other agencies will not meet all of these deadlines. For example, the DHS has not selected a Federal dashboard to report ISCM program metrics. The DHS has also set a schedule into FY 2015 for agencies and vendors to meet in private to determine individual solutions for their ISCM programs.

Despite the Federal delay in ISCM program implementation, the IRS must be in compliance with both Treasury Department and OMB guidelines for its ISCM program. The IRS has been participating along with other bureaus in Treasury Department meetings on the ISCM program and in DHS training. The IRS has satisfied OMB requirements for agencies that include:

- Creating a strategy to implement the ISCM program.
- Identifying specific individuals to manage the agency's ISCM program.
- Identifying resource and skill requirement gaps to manage and coordinate the internal ISCM program.
- Coordinating with the Treasury Department on the CDM program foundational survey that was sent to the DHS and signing the Treasury Department Memorandum of Agreement with the DHS.[4]

The IRS has many tools in place for Phase 1 of the ISCM program that sustain current controls for identifying security vulnerabilities. The IRS is taking the initiative to enhance its current tools and is planning the integration of a comprehensive, enterprise-wide information technology service management solution that includes the Enterprise Configuration Management System; the Knowledge, Incident, Service Asset Management System; the End-2-End Monitoring and Event Management System; and the Work Request Management System. By following the

[4] See Appendix V for the OMB deadlines.

Information Technology Infrastructure Library Process Model,[5] the IRS will be creating a more robust system by integrating asset management, configuration management, change management, and service management.

Moving forward, the IRS should implement an internal dashboard

It is the DHS's responsibility to establish a Federal dashboard for the ISCM program, which will provide a Governmentwide view of the ISCM program as well as the technical specifications and guidance for agencies on the requirements for submitting information to this Federal dashboard. However, the security-related information gathered for input to the Federal dashboard will not provide the comprehensive information required to make risk-based decisions about the effectiveness of all selected and implemented security controls by the agencies. Additional security-related information will be needed to make fully informed risk-based decisions regarding specific information systems. Therefore, an internal IRS dashboard or similar tool would give a comprehensive view of all the systems, and not just the metrics reported to the Federal dashboard, so that risk-based decisions can be made when security vulnerabilities arise.

With the release of the IRS's ISCM Strategy document, the Treasury Department has been a constant guide throughout the ISCM program process. In October 2013, the Treasury Department issued a memorandum stating that a continuous monitoring dashboard would be used at the Treasury Department level for all bureaus, which would save the bureaus the expense of having to purchase their own dashboard. The dashboard will remain at the Treasury Department's Government Security Operations Center, and all Treasury Department bureaus will feed information from each of the security automation domains into this dashboard.

The DHS is responsible for the purchase and rollout of the Federal dashboard for the ISCM program that will include both Federal and agency-level metrics for the entire Federal Government. However, the DHS has not selected a dashboard product. Based on DHS coordination, Treasury Department officials have estimated that the selection of a Federal dashboard and the completion of Phase 1 of the ISCM program implementation will not be known until the third quarter of FY 2015.

Although the IRS has many security tools in place to satisfy the requirements for Phase 1 of the ISCM program, the reports from these tools are sent to various dashboards or directly to stakeholders and not to a single dashboard that could provide consistency in reporting and allow decision makers to see a comprehensive view. Without a main control point for consolidating security tool metrics, critical information necessary for making risk-based decisions may be overlooked, and according to OMB Memorandum 14-03, all agencies are ultimately responsible for security vulnerabilities within their agencies. The OMB has set specific ISCM program

[5] The Information Technology Infrastructure Library is a set of practices for information technology service management that focuses on aligning information technology services with the needs of business. It is used to demonstrate compliance and to measure improvement, including a process model that organizations can use for implementing their practices.

implementation deadlines for the agencies once the DHS dashboard is selected. The following deadlines are dependent on the Federal dashboard being selected:

- Ensure that all Phase 1 products necessary to meet DHS reporting requirements provide data compatible with the Federal dashboard maintained by the DHS.
- Complete installation of agency- and bureau/component-level dashboards.
- Begin submitting automated data feeds for Phase 1 focus areas to the Federal dashboard.

Although the IRS has not selected a dashboard for its ISCM program, it has options for the selection. Currently, the IRS is implementing a business management tool, RSA Archer enterprise Governance Risk and Compliance (eGRC),[6] which will be used as a compliance dashboard. Although the Treasury Inspector General for Tax Administration (TIGTA) did not evaluate the RSA Archer eGRC as a risk-based dashboard, it is a viable option according to the IRS. The Cybersecurity office selected the RSA Archer eGRC because of its high rating by Gartner as an eGRC tool, and since the IRS's selection, the DHS has included it in its BPA. Risk prioritization is an area that will eventually be portrayed in the RSA Archer eGRC. It will help management quantify various risks based on the critical level of the system or server.

The IRS currently uses the RSA Archer eGRC platform that monitors contractor training, and TIGTA and Government Accountability Office reviews. The IRS has also begun piloting the integration of a scanning tool into the RSA Archer eGRC so that the metrics of this tool can be rolled up directly into the dashboard. This dashboard could be used for the IRS's ISCM program to support risk-based decisions by stakeholders to assess the vulnerabilities identified by the security scanning tools.

During our review, funding for the RSA Archer eGRC was approved to obtain more server capacity. However, as tools are integrated into the dashboard, whether for the ISCM program or compliance monitoring, server capacity could be a future problem and may prohibit the integration of more scanning tools into the dashboard, which could limit the amount of metrics and affect stakeholders' decisions if the metrics do not include all systems or mitigating factors.

As another option, the IRS has access to the GSA's BPA through the DHS CDM program. The IRS is able to select a dashboard from the BPA if it better meets its internal requirements. Although the Treasury Department foresees that the Federal dashboard will not be selected until well into FY 2015, the IRS may find a more cost-efficient interim dashboard while waiting for the Federal selection in the upcoming fiscal year.

Although the Treasury Department has issued Treasury Chief Information Officer Memorandum 14-02, *Standard Tool Selection for Automated Information Security Continuous*

[6] RSA Archer eGRC is a flexible enterprise eGRC framework application that allows organizations to tailor their unique requirements, create supporting applications, and integrate multiple data sources without touching a single line of code.

Monitoring (ISCM), stating that there will be one dashboard to report ISCM program metrics for the Treasury Department, Treasury Department officials agreed that given the size and complexity of the IRS's computer environment, an IRS internal dashboard would give IRS stakeholders a comprehensive view of the status of IRS systems, allowing for a more secure environment. As a courtesy, the IRS should coordinate with Treasury Department officials on the selection of its internal dashboard and the metrics integration with the Treasury Department dashboard.

Recommendation

The Chief Technology Officer should continue to move forward and coordinate, as appropriate, with the Treasury Department to implement a stronger internal ISCM program that allows executives to make the most informed decisions that affect the security of the IRS network by taking the following action.

Recommendation 1: The Chief Technology Officer should select and implement an integrated dashboard of the security scanning tools to allow stakeholder and decision makers to make well-informed risk-based decisions.

> ***Management's Response:*** The IRS agreed with our recommendation. The Chief Technology Officer will select and implement an integrated dashboard of the security scanning tools to allow stakeholders and decision makers to make well-informed risk-based decisions by establishing an enterprise-wide integrated project team to direct the IRS's ISCM initiative. Based on the future direction of the ISCM integrated project team, the IRS will select and implement an integrated, local dashboard of its security scanning tools.

The Internal Revenue Service Should Leverage the Blanket Purchase Agreement to Acquire Security Tools Needed for Its Environment

As the largest agency within the Treasury Department, the IRS has numerous systems and platforms to administer the Nation's tax system. Compared with other Treasury Department bureaus, the IRS has far more systems and software, many of which dwarf other Treasury Department bureaus' systems, with 150 FISMA reportable Major Applications and General Support Systems,[7] more than 7,000 servers, and more than 100,000 workstations. In addition,

[7] The FISMA requires agencies to develop and maintain an inventory of major information systems operated by or under the control of the agency. The FISMA considers the following as "reportable" information systems: 1) the General Support System is an interconnected set of information resources under the same direct management control that shares common functionality and normally includes hardware, software, information, data, applications, communications, and people and 2) the Major Application is an application that requires special attention to security due to the risk and magnitude resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.

the IRS's computer environment is complex and varied, with different software and hardware products for various computer components. To require an agency with approximately 93,000 employees and with responsibility for millions of taxpayer records to include the purchasing of tools in a one-size-fits-all process may not be the best approach for the IRS and could possibly slow any progress on the implementation of the ISCM program and result in the risk of allowing gaps in the security of critical systems.

As such, the IRS has security tools in place that address the first three security automation domains required in Phase 1 and the Patch Management security automation domain as well. With a complex computer environment that includes various network devices, applications, databases, hardware, software, middleware, and operating system platforms, the IRS may need to use more than one type of security tool for identifying, tracking, and preventing vulnerabilities. These tools are an integral part of identifying security vulnerabilities over the IRS's numerous systems and networks.

In efforts to ensure that the bureaus are compliant with the ISCM program as required by the OMB, the Treasury Department is spearheading the implementation by holding periodic meetings with the bureaus to streamline the tool selection for each of the security automation domains in Phase 1. The Treasury Department has been collecting information from the various bureaus regarding the ISCM program tools to be used to fulfill DHS's Task Order 1 of the CDM program and the three security automation domains of Phase 1 outlined in the Joint Continuous Monitoring Working Group's CONOPS document released in 2013.

DHS's Task Order 1 includes the three security automation domains identified in the CONOPS as Asset Management broken down as Hardware and Software Asset Management, Configuration Management, and Vulnerability Management. Task Order 1 also identifies web and code scanning tools.

The OMB issued a memorandum dated November 2013 that outlines the due dates for the following year for every agency and the parameters that must be met in implementing the ISCM program. In addressing gaps, agencies should leverage, to the extent practicable, the GSA BPA. As stated in the memorandum and outlined in the CONOPS, agencies have the discretion to implement the tools necessary for their ISCM program technical architecture.

1. Leveraging the services and products offered by the DHS CDM program;
2. Leveraging the agency's existing products and services; and/or
3. Implementing a hybrid approach by which agencies can leverage the DHS CDM program to procure products but implementing it using their own hardware.

For consistency, the Treasury Department is mandating bureaus use the tool it selected for official reporting for the ISCM program, even if another tool is better suited for a specific environment or performs the same function as the mandated tool. The Treasury Department stated that the purpose of this request is to have all information consistent among the bureaus

when feeding information to the dashboard at the Treasury Department. With the variety of tools offered by numerous vendors, Treasury Department officials are working to coordinate with bureaus to streamline the selection process. However, this process and purchasing of tools has been slow at best. Currently, Treasury Department officials have selected only one tool for Phase 1.

On March 25, 2014, the Treasury Department issued Treasury Chief Information Officer Memorandum 14-02 on CDM program tool standardization. The memorandum states that when the procurement process is completed and tools are selected, the Treasury Department standard mandatory CDM program tools will be deployed across bureau infrastructures either by a DHS service provider/integrator or by the bureaus themselves. Treasury Department officials have collected these preferences from each bureau already. The bureaus will be responsible for the operation of the CDM program tools deployed in their environments. The bureaus may continue to supplement the Treasury Department standard tools with their own security tools, provided that the Treasury Department standard CDM program tools retain budgetary priority and are free of technical interference from the bureaus' tools.

Although efforts to streamline tools for efficiency and consistency could be possible, security should take precedence and is the backbone to the ISCM program. After discussing the inherent risks associated with the overall size of the IRS and the numerous systems containing taxpayer information, Treasury Department officials agreed that security should be the main priority, and not consistency, when implementing an ISCM program. To assist in this effort, the Treasury Department suggested that the IRS leverage the BPA to acquire the tools necessary for identifying security vulnerabilities in the IRS environment. Treasury Department officials requested that the IRS coordinate with them when acquiring tools to determine the best cost savings.

Inefficiencies could result if the IRS selects the recommended Treasury Department tool

In the fall of 2013, the Treasury Department selected DbProtect as the official tool for database scanning for the bureaus. The Treasury Department requested 5,000 licenses of DbProtect through the DHS's BPA with the GSA. Of the licenses requested, the DHS informed the Treasury Department that it would only receive 950 licenses. As a result, the Treasury Department will need to determine which bureaus will receive licenses and the approximate number for each.

Through discussions with IRS officials, we were informed that the IRS has moved away from DbProtect and is now using Guardium for its database scanning. Although neither product was an "out-of-the-box"[8] solution, according to the IRS, Guardium appeared to be the more practical

[8] Out-of-the-box feature or functionality, particularly in software, is a feature or functionality of a product that works immediately after installation without any configuration or modification. In this situation, the IRS would need to configure the software to make it a viable solution for its environment.

and cost-effective choice for IRS mainframe database scanning. The IRS has invested significant resources in Guardium over the last three years to make it suitable to the IRS scanning environment.

If the IRS were to stop using Guardium and renew a contract with DbProtect, it would have wasted considerable funds to adapt Guardium as a database scanning tool, including the time and effort attributed to making the Guardium product a workable solution. Furthermore, additional time and resources would be required to make DbProtect a capable solution, with no assurance that it will be comparable to that of Guardium.

Requiring the IRS to adopt a technology that does not best suit its security environment could inhibit its ability to implement a robust ISCM program strategy and potentially force the IRS to invest additional time and resources in order to comply with Treasury Department requirements. To require that the IRS purchase and maintain more than one tool to scan the same operating system is an inefficient use of resources.

The IRS lacks an enterprise-wide software management system

The IRS does not have an enterprise-wide software management system. As part of Phase 1 of the ISCM program, the Asset Management security automation domain includes Software Asset Management. Although the IRS's ISCM Strategy document states that the IRS has tools to identify or discover software on the networks, we found that an enterprise-wide management system for software was not in place.

In prior TIGTA reviews[9] addressing workstations, servers, and mainframes, TIGTA found that the IRS lacks an enterprise-wide repository and organizational structure for software management. The IRS has not invested in the resources to develop and implement an effective software asset management program. In response to TIGTA's reports, the IRS stated that one tool cannot possibly track, discover, and manage software. Therefore, the IRS is currently working on a toolkit to implement an enterprise-wide software management program. In addition, a recently completed MITRE Corporation gap and overlap security tool analysis for the IRS found that the IRS lacks tools for detecting unauthorized software and security setting compliance on perimeter firewalls and proxies, wireless access points, and handheld devices.

According to DHS training, the purpose of software asset management is to identify unauthorized software on devices that is likely to be used by attackers as a platform from which to extend compromise of the network. Security scans should target software products and executables (individual program files). Agencies should maintain a list of authorized software at both the product and executable level and treat other software actually on the network as a

[9] TIGTA, Ref. No. 2013-20-025, *Desktop and Laptop Software License Management Is Not Being Adequately Performed* (June 2013); TIGTA, Ref. No. 2014-20-002, *The Internal Revenue Service Should Improve Mainframe Software Asset Management and Reduce Costs* (Feb. 2014); and TIGTA, Ref. No. 2014-20-042, *The Internal Revenue Service Should Improve Server Software Asset Management and Reduce Costs* (Sept. 2014).

defect. The agency should remove, authorize/assign, or accept the risk for the other software classified as a defect.

The IRS needs tools to cover gaps for the ISCM Software Asset Management security automation domain. Without the necessary security tools to detect and remove unauthorized software, the IRS is vulnerable to security risks and the exploitation of IRS systems.

The IRS should enhance security tools currently in use

Currently, the IRS is using many security tools required for Phase 1 of the ISCM program to address the first three security automation domains, such as a database scanning, web and code scanning, laptop and server configuration scanning, unauthorized hardware and software scanning, and security network scanning. However, the IRS discovered that these tools may need additional resources to enrich the current tool capability. The IRS has the option to use the BPA to improve the security of its ISCM program by enhancing tools already in use.

Some of these tools could also be used in a broader sense; for example, one of the security tools that the IRS owns is BDNA Technopedia Discover™[10] for asset discovery. However, the part of BDNA that could be enhanced is BDNA Normalize.™ Normalize will allow raw data to be recognized in a common language between systems. Normalize also aligns and updates inconsistent data such as vendor names, product names, product version, *etc*., to provide a consistent view into data across multiple information technology systems. With Normalize, the IRS could enhance the language between the BDNA tool and another IRS scanning tool currently in use to compare the scanning results of assets. The IRS could take advantage of the BPA to acquire the additional software to connect the two scanning tools. By enhancing the tools, the data are easily recognized and shared between the tools in a common way, thereby allowing stakeholders to make informed risk decisions.

Security will be improved by enhancing the existing tools and adding additional resources for the tools to operate optimally. Without these enhancements, the tools could allow vulnerabilities that might otherwise be identified and mitigated.

Recommendations

The Chief Technology Officer should:

Recommendation 2: Take advantage of the GSA BPA through the DHS's CDM program to acquire products to ensure that gaps in coverage and tool enhancements of the ISCM program are adequately addressed and best suited for the IRS environment.

[10] Technopedia Discover can scan assets across multiple data centers and firewall zones. It quickly discovers, identifies, and categorizes more than 450,000 types of hardware and software products to provide trusted, complete, and enriched information technology inventory information.

Management's Response: The IRS agreed with our recommendation. The Chief Technology Officer will take advantage of the GSA BPA to acquire products to ensure that gaps in coverage and tool enhancements are adequately addressed and best suited for the IRS environment. The Chief Technology Officer will establish an enterprise-wide integrated project team to direct the IRS's ISCM initiative. Based on the future direction of the ISCM integrated project team and the tools analysis already completed, the IRS will pursue tool enhancements for current tools and tool selections for gaps in the most efficient method to the extent funding is available.

Recommendation 3: Continue to coordinate with the Treasury Department to ensure that the tools selected for use (including the database scanning tool) are the most effective and make the most efficient use of IRS resources.

Management's Response: The IRS agreed with our recommendation. The Chief Technology Officer will continue to coordinate with Treasury to ensure that the IRS selects the most effective and efficient security tools in terms of cost and to fully ensure that all unique technical needs within the IRS computing environment are addressed.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to assess the current state of CDM program controls in place at the IRS. To accomplish our overall goal, we:

I. Determined whether CDM program controls surrounding the Asset Management security automation domain were working as intended.

- A. Determined the current state of CDM program controls for the Asset Management security automation domain and whether the current controls are effective and compliant with applicable guidance.
- B. Determined whether proposed CDM program controls and the timeline for implementation of these controls are compliant with applicable guidance.

II. Determined whether CDM program controls surrounding the Configuration Management security automation domain are working as intended.

- A. Determined the current state of CDM program controls for the Configuration Management security automation domain.
- B. Determined whether proposed CDM program controls and the timeline for implementation of these controls are compliant with applicable guidance.

III. Determined whether CDM program controls surrounding the Patch Management security automation domain are working as intended. (Note: This security automation domain was not a part of Phase 1 mandated by the OMB. Although we reviewed this area because it was in the IRS's strategy, we did not report on this test.)

- A. Determined the current state of CDM program controls for the Patch Management security automation domain.
- B. Determined whether proposed CDM program controls and the timeline for implementation of these controls are compliant with applicable guidance.

IV. Determined whether CDM program controls surrounding the Vulnerability Management security automation domain are working as intended.

- A. Determined the current state of CDM program controls for the Vulnerability Management security automation domain.
- B. Determined whether proposed CDM program controls and the timeline for implementation of these controls are compliant with applicable guidance.

V. Assessed the timing for full implementation of the CDM program.

A. Determined whether the IRS has received appropriate guidance from the Department of the Treasury.

B. Determined whether the IRS has made adequate progress in development of the remaining security automation domains.

C. Determined any setbacks and hurdles experienced in implementing the CDM program.

D. Determined how the future-state vendors will be selected and assessed the potential for fraudulent manipulation of this process by the IRS.

E. Determined the status of the remaining seven security automation domains.

Internal controls methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: the OMB, the Joint Continuous Monitoring Working Group's CONOPS, the NIST, and the Treasury Department guidelines for continuous monitoring and the IRS's efforts to implement these controls in order to determine near real-time security of the IRS networks and data to allow ongoing authorizations and risk-based decisions. We evaluated these controls by conducting interviews and meetings, observing tools, and reviewing documentation with cybersecurity management and business owners at the IRS responsible for securing the Asset Management, Configuration Management, and Vulnerability Management security automation domains.

Appendix II

Major Contributors to This Report

Alan Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Director
Joseph F. Cooney, Audit Manager
Cari Fogle, Lead Auditor
Midori Ohno, Senior Auditor
Sam Mettauer, Information Technology Auditor

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Deputy Chief Information Officer for Operations OS:CTO
Associate Chief Information Officer, Cybersecurity OS:CTO:C
Associate Chief Information Officer, Enterprise Operations OS:CTO:EO
Associate Chief Information Officer, Enterprise Services OS:CTO:ES
Associate Chief Information Officer, User and Network Services OS:CTO:UNS
Director, Security Risk Management OS:CTO:C:SRM
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

National Institute of Standards and Technology Security Automation Domains

Security Automation Domain	***Description***
Asset Management	Asset management tools help maintain inventory of software and hardware within the organization. This can be accomplished via a combination of system configuration, network management, and license management tools or with a special-purpose tool. *NOTE: The CONOPS defines this area as Hardware Asset Management and Software Asset Management and makes them two separate domains, which equal four domains for Phase 1.*
Vulnerability Management	A vulnerability is a software flaw that introduces a potential security exposure. Vulnerability scanners are commonly used in organizations to identify known vulnerabilities on hosts and networks and on commonly used operating systems and applications. These scanning tools can proactively identify vulnerabilities, provide a fast and easy way to measure exposure, identify out-of-date software versions, validate compliance with an organizational security policy, and generate alerts and reports about identified vulnerabilities. *NOTE: The CONOPS includes this domain in Phase 1.*
Configuration Management	Configuration management tools allow administrators to configure settings, monitor changes to settings, collect setting status, and restore settings as needed. *NOTE: The CONOPS includes this domain in Phase 1.*
Patch Management	Patch management tools scan for vulnerabilities on systems and system components participating in an organization's patching solution, provide information regarding needed patches and other software updates on affected devices, and allow an administrator to decide on the patching implementation process.
Event Management	Event management involves monitoring, and responding to as necessary, observable occurrences in a network or system. A variety of tools and technologies exist to monitor events, such as intrusion detection systems and logging mechanisms. Some tools may detect events based on known attack signatures, while others detect anomalies in behavior or performance that could indicate an attack.

Security Automation Domain	*Description*
Incident Management	Certain events may signal that an incident has occurred, which is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. Incident management tools may assist in detecting, responding to, and limiting the consequences of a malicious cyberattack against an organization.
Malware Detection	Malware detection provides the ability to identify and report on the presence of viruses, Trojan horses, spyware, or other malicious code on or destined for a target system.
Network Management	Network configuration management tools include host discovery, inventory, change control, performance monitoring, and other network device management capabilities. Some network configuration management tools automate device configuration and validate device compliance against preconfigured policies. Network management tools may be able to discover unauthorized hardware and software on the network, such as a rogue wireless access point.
License Management	Similar to systems and network devices, software and applications are also a relevant data source for the ISCM program. Software asset and licensing information may be centrally managed by a software asset management tool to track license compliance, monitor usage status, and manage the software asset life cycle. License management tools offer a variety of features to automate inventory, utilization monitoring and restrictions, deployment, and patches for software and applications.
Information Management	There are vast quantities of digital information stored across the myriad of systems, network devices, databases, and other assets within an organization. Managing the location and transfer of information is essential to protect the confidentiality, integrity, and availability of the data.
Software Assurance	The NIST Software Assurance Metrics and Tool Evaluation project defines software assurance as the "planned and systematic set of activities that ensures that software processes and products conform to requirements, standards, and procedures from NASA Software Assurance Guidebook and Standard to help achieve: (1) Trustworthiness – No exploitable vulnerabilities exist, either of malicious or unintentional origin (2) Predictable Execution – Justifiable confidence that software, when executed, functions as intended."

Appendix V

Office of Management and Budget Deadlines

	Required Action	*Deadline*	*Responsible Entity*	*IRS Status*
1	Develop ISCM program strategy (or strategies).	February 28, 2014.	All agencies.	Completed August 9, 2013.
2	Identify resource and skill requirement gaps (if any) to manage and coordinate the internal ISCM program.	April 30, 2014.	All agencies.	Completed April 30, 2014.
3	Identify specific individuals to manage the agency's ISCM program.	April 30, 2014.	All agencies.	Completed April 14, 2014.
4	Complete the CDM program foundational survey and return to the DHS.	Immediately, if not already completed.	All civilian agencies.	Completed survey of data tools. Sent to the Treasury Department on December 3, 2013.
5	Sign Memorandum of Agreement with the DHS.	Immediately, if not already completed.	All civilian agencies receiving DHS CDM program services.	The Treasury Department is in contact on behalf of the IRS.
6	Begin to procure products and services to support Phase 1 focus areas (as described in the CONOPS).	February 28, 2014.	All agencies.	Satisfied by the Treasury Department by purchase of DbProtect for bureaus in Fall 2013. Also, the DHS has pushed the meetings with vendors into FY 15.

	Required Action	*Deadline*	*Responsible Entity*	*IRS Status*
7	Begin to deploy products to support ISCM for all systems.	May 30, 2014.	All agencies.	Completed; the IRS already has products in deployment.
8	Ensure that all information systems are authorized to operate in accordance with Federal requirements prior to initiating ISCM for those systems.	May 30, 2014.	All agencies.	Completed; the information systems for Phase 1 at the IRS have authorization to operate.
9	Publish technical specifications for agency data feeds for Phase 1 focus areas to the Federal dashboard.	Three months prior to deployment of the Federal dashboard.	The DHS.	N/A.
10	Ensure that all Phase 1 products necessary to meet DHS reporting requirements provide data compatible with the Federal dashboard maintained by the DHS.	Within three months of the Federal dashboard being deployed.	All agencies.	To be determined.
11	Complete installation of agency- and bureau/component-level dashboards.	Within six months of the Federal dashboard being deployed.	All agencies.	To be determined.
12	Begin submitting automated data feeds for Phase 1 focus areas to the Federal dashboard.	Within six months of the Federal dashboard being deployed.	All agencies.	To be determined.
13	Publish guidance establishing a process and criteria for agencies to conduct ongoing assessments and authorizations.	March 31, 2014.	The NIST.	Issued June 2014.

	Required Action	***Deadline***	***Responsible Entity***	***IRS Status***
14	Update ISCM program strategies to describe the process for performing ongoing authorizations.	Within three months of receiving additional guidance in this area (either from the NIST, the DHS, and/or the Joint Continuous Monitoring Working Group).	All agencies.	In progress.
15	Determine whether agencies have documented their ISCM program strategy.	November 15, 2014 (and each year thereafter).	Inspectors General.	Completed August 2013.
16	Assess whether agencies have implemented ISCM for information technology assets.	November 15, 2014 (and each year thereafter).	Inspectors General.	To be determined.
17	Evaluate agencies' risk assessments used to develop their ISCM program strategy.	November 15, 2014 (and each year thereafter).	Inspectors General.	To be determined.
18	Verify that agencies conduct and report on ISCM program results in accordance with their continuous monitoring strategy.	November 15, 2014 (and each year thereafter).	Inspectors General.	To be determined.

Appendix VI

Management's Response to the Draft Report

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

CHIEF TECHNOLOGY OFFICER

AUG 2 8 2014

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Terence V. Milholland
Chief Technology Officer

SUBJECT: Draft Audit Report – The Internal Revenue Service Should Implement an Efficient, Internal Information Security Continuous Monitoring Program That Meets Its Security Needs, (Audit # 201320003) (e-trak #2014-58147)

Thank you for the opportunity to review your draft audit report and meet with the audit team to discuss earlier report observations. We are pleased that your report acknowledged the IRS is making progress in implementing the Information Security Continuous Monitoring program. The Agency is taking initiatives by enhancing our current tools and is planning the integration of a comprehensive, enterprise-wide information technology service management solution.

The IRS is committed to continuously improving the Information Security Continuous Monitoring Program and monitoring security controls of our computer assets in real time; thusly, improving the effectiveness and safeguards of taxpayer information and information systems. The attachment to this memo details our planned corrective actions to implement the audit report's recommendations.

The IRS values your continued support and the assistance your organization provides. If you have any questions, please contact me at (240) 613-9373 or John Allen, Director of Risk Management, at (202) 317-5594.

Attachment

Draft Audit Report –The Internal Revenue Service Should Implement an Efficient, Internal Information Security Continuous Monitoring Program That Meets Its Security Needs (Audit # 201320003) (e-trak #2014-58147)

RECOMMENDATION #1: The Chief Technology Officer should, select and implement an integrated dashboard of the security scanning tools to allow stakeholder and decision makers to make well informed risk based decisions.

CORRECTIVE ACTION #1: The Chief Technology Officer (CTO) will select and implement an integrated dashboard of the security scanning tools to allow stakeholders and decision makers to make well informed risk based decision by establishing an enterprise-wide integrated project team (IPT) to direct our information security continuous monitoring (ISCM) initiative. Based on the future direction of the ISCM IPT, the IRS will select and implement an integrated, local, dashboard of its security scanning tools.

IMPLEMENTATION DATE: July 25, 2016

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #2: The Chief Technology Officer should, take advantage of the GSA BPA through the DHS's CDM program to acquire products to ensure that gaps in coverage and tool enhancements of the ISCM program are adequately addressed and best suited for the IRS environment.

CORRECTIVE ACTION #2: The Chief Technology Officer (CTO) will take advantage of the GSA BPA to acquire products to ensure gaps in coverage and tool enhancements are adequately addressed and are best suited for the IRS environment. The CTO will establish an enterprise-wide integrated project team (IPT) to direct our information security continuous monitoring (ISCM) initiative. Based on the future direction of the ISCM IPT, and from the tools analysis already completed, the IRS will pursue tool enhancements, for current tools, and tool selections, for gaps, in the most cost-efficient method. To the extent funding is available.

IMPLEMENTATION DATE: January 25, 2015

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

Draft Audit Report –The Internal Revenue Service Should Implement an Efficient, Internal Information Security Continuous Monitoring Program That Meets Its Security Needs (Audit # 201320003) (e-trak #2014-58147)

RECOMMENDATION #3: The Chief Technology Officer should, continue to coordinate with Treasury to ensure that the tools selected for use (including the database scanning tool) is the most effective and makes the most efficient use of IRS resources.

CORRECTIVE ACTION #3: The Chief Technology Officer will continue to coordinate with Treasury to ensure that the IRS selects the most effective and efficient security tools in terms of cost and to fully ensure all unique technical needs within the IRS computing environment are addressed.

IMPLEMENTATION DATE: January 25, 2015

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.