Significant Delays Hindered Efforts to Provide Continuous Monitoring of Security Settings on Computer Workstations

January 24, 2013

Reference Number: 2013-20-016

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

SIGNIFICANT DELAYS HINDERED EFFORTS TO PROVIDE CONTINUOUS MONITORING OF SECURITY SETTINGS ON COMPUTER WORKSTATIONS

Highlights

Final Report issued on January 24, 2013

Highlights of Reference Number: 2013-20-016 to the Internal Revenue Service Chief Technology Officer.

IMPACT ON TAXPAYERS

Effective continuous monitoring of computer workstations allows security issues to be identified and mitigated promptly, reducing the likelihood of a security breach. When IRS data and its network are not secured, taxpayer information becomes vulnerable to unauthorized disclosure and theft. Furthermore, security breaches can cause network disruptions and prevent the IRS from performing vital taxpayer services, such as processing tax returns, issuing refunds, and answering taxpayer inquires. In addition, the IRS collects vast quantities of personal and financial information that can be targeted for identity theft.

WHY TIGTA DID THE AUDIT

The overall objective of this review was to determine whether the IRS is effectively and efficiently implementing its continuous monitoring tool to monitor security settings on employee workstations and laptop computers. This audit was included in TIGTA's Fiscal Year 2012 Annual Audit Plan and addresses the major management challenge of Security for Taxpayer Data and Employees.

WHAT TIGTA FOUND

The Treasury Enhanced Security Initiatives project, which includes the continuous monitoring tool for workstation security, will address several computer security weaknesses. The IRS appropriately acquired the project's multiple software components, and the project team completed key documentation during the development process, ensuring that critical issues were identified and addressed. However, the Treasury Enhanced Security Initiatives project has experienced several delays, and the project's oversight board did not take required actions to manage the delays or the associated costs. The IRS was scheduled to deploy the security tools in December 2010 but now plans to complete the deployment in May 2013.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Technology Officer direct the Cybersecurity and Privacy Governance Board to: 1) review total actual life cycle costs for projects at least quarterly and review variances between actual costs and the originally proposed estimated costs, 2) manage costs by considering the postponement of projects with long-term delays, and 3) escalate ongoing project delays to the higher level Security Services and Privacy Executive Steering Committee.

The IRS agreed with TIGTA's recommendations and plans to review information technology projects' life cycle costs, consider postponing those projects with long-term delays, and escalate delays to the higher level Security Services and Privacy Executive Steering Committee.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

January 24, 2013

MEMORANDUM FOR CHIEF TECHNOLOGY OFFICER

Nancy A. Nakamura

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

SUBJECT: Final Audit Report – Significant Delays Hindered Efforts to Provide Continuous Monitoring of Security Settings on Computer Workstations (Audit # 201220008)

This report presents the results of our review of the Internal Revenue Service's (IRS) continuous monitoring efforts on computer workstations. The overall objective of this review was to determine whether the IRS is effectively and efficiently implementing its continuous monitoring tool to monitor security settings on employee workstations and laptop computers. This audit was included in the Treasury Inspector General for Tax Administration's Fiscal Year 2012 Annual Audit Plan and addresses the major management challenge of Security for Taxpayer Data and Employees. This audit was also part of our statutory requirement to annually review the adequacy and security of IRS technology.

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

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 Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Abbreviations

FDCC	Federal Desktop Core Configuration
IRS	Internal Revenue Service
IT	Information Technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
SCAP	Secure Content Automation Protocol
SRAS	Symantec Risk Automation Suite
TESI	Treasury Enhanced Security Initiatives
TIGTA	Treasury Inspector General for Tax Administration

Background

Government computer systems are subject to a variety of threats. According to the Government Accountability Office, cyber-based[1] threats to Federal systems and critical infrastructure are evolving and growing.[2] These threats can be intentional or unintentional, targeted or nontargeted, and come from a variety of sources, including criminals, terrorists, and other adversarial groups, as well as hackers and disgruntled employees. The motivations for these threats—both external and internal—include causing disruption, committing fraud, and performing identity theft. Security protections cannot prevent all attacks, but they can reduce the opportunities that attackers have to gain access to a computer or to damage the computer's software or information. At the Internal Revenue Service (IRS), security breaches can cause network disruptions and prevent the IRS from performing vital taxpayer services, such as processing tax returns, issuing refunds, and answering taxpayer inquires. In addition, the IRS collects vast quantities of personal and financial information that can be targeted for identity theft. Security settings on computer systems should be monitored and maintained continuously so that security weaknesses can be identified and mitigated promptly, reducing the likelihood of a security breach. When IRS data and its network are not secured, taxpayer information becomes vulnerable to unauthorized disclosure and theft.

In March 2007, the Office of Management and Budget (OMB) launched the Federal Desktop Core Configuration (FDCC) initiative,[3] setting forth requirements for establishing standard secure configurations on Federal workstations running the Windows® Vista and Windows XP operating systems. The FDCC was later updated to include security configuration settings for the Windows 7 operating system. Two main goals of the FDCC are to improve information security and reduce overall information technology operating costs by providing a baseline level of security configuration settings. When these settings are maintained on computer systems, less time and money is spent eradicating malware, restoring systems from backups, and reinstalling operating systems and applications. A reduction in vulnerability exposure is also achieved.

The IRS is required to continuously monitor security settings on computer workstations to identify and address security settings that have been altered.

[1] See Appendix VI for a glossary of terms.
[2] Government Accountability Office, GAO-10-202, *Agencies Need to Implement Federal Desktop Core Configuration Requirements*, 3 (2010).
[3] Office of Management and Budget, OMB Memorandum M-07-11, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems* (2007).

The OMB required agencies to implement the standard security configurations by February 2008 and to begin continuous monitoring of these settings in August 2008.[4] The OMB required agencies to monitor the security settings by using a Secure Content Automation Protocol (SCAP)-validated tool with FDCC scanner capability. The tool must be validated by the National Institute of Standards and Technology (NIST).

The SCAP approach provides an automated, standardized approach to maintaining the security of enterprise systems, such as implementing security configuration baselines, verifying the presence of patches, performing continuous monitoring of system security configuration settings, examining systems for signs of compromise, and achieving situational awareness, *i.e.,* being able to determine the security posture of systems and the organization at any given time.

The IRS is currently addressing the OMB mandates with a tool developed by the Space and Naval Warfare Systems Command called the SCAP Compliance Checker. However, this tool has limited functionality, and the IRS is attempting to replace it with more robust technology. These efforts are managed through the IRS's Treasury Enhanced Security Initiatives (TESI) project. The TESI project is led by officials in the Information Technology (IT) organization's User and Network Services function. Oversight is provided by the Cybersecurity and Privacy Governance Board, which oversees nonmajor information technology projects and is responsible for ensuring project objectives are met, risks are managed appropriately, and expenditures are fiscally sound.[5]

This review was performed at the IRS IT organization offices in New Carrollton, Maryland, and in the Treasury Inspector General for Tax Administration (TIGTA) office in Dallas, Texas, during the period January through August 2012. 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 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.

[4] Office of Management and Budget, OMB Memorandum M-08-22, *Guidance on the Federal Desktop Core Configuration* (2008).
[5] Within the IRS IT organization, the following functions have voting representatives on the Cybersecurity and Privacy Governance Board: Applications Development, Cybersecurity, (Architecture and Implementation, Operations, and Risk Management Divisions), User and Network Services, Enterprise Operations, and Enterprise Services.

Results of Review

The Treasury Enhanced Security Initiatives Project Will Address Several Computer Security Weaknesses on Employee Workstations

The SCAP Compliance Checker tool currently being used to monitor security settings allows the IRS to achieve a minimum level of compliance with the FDCC mandate. The tool scans for FDCC settings and is SCAP-compliant, based on the initial version of the tool that was certified by the NIST. However, this compliance checker tool lacks significant capabilities. Specifically, the tool:

- Does not provide remediation capabilities.
- Does not generate reports that present specific FDCC setting deficiencies.
- Does not allow the IRS to identify which workstations have noncompliant configurations or which configurations have been improperly altered.

Knowing which security settings have been altered on specific computers is crucial because some settings are more significant than others and require immediate attention. For example, one FDCC setting restricts the undocking of a laptop computer from its docking station. Laptop computers are designed to be undocked for travel and teleworking purposes. For this reason, the undocking security setting is not as significant as others. The IRS would not prioritize fixing this low-risk setting if it was altered on a computer workstation. By contrast, another FDCC setting that blocks users from downloading malicious programs or installing devices onto their workstations is significant and the IRS would prioritize the investigation of changes to this setting. The IRS needs an automated monitoring tool with the capability to identify and report both the specific noncompliant FDCC settings and the workstations that contain the noncompliant settings.

The objective of the TESI project is to enable the IRS to fully comply with the OMB mandate and implement other key security controls for workstations. The TESI project will be deployed in two phases and includes six separate software components. The first phase of the project includes three components:

- The Symantec Risk Automation Suite (SRAS) will use dissolving agents to scan security configurations on computer workstations and identify noncompliant settings on specific workstations. The SRAS tool, once deployed, will perform asset discovery, auditing, and reporting for all IRS workstations. The SRAS will analyze workstations for policy compliance as determined by the FDCC, the NIST, and internal IRS policies. This component will also allow the IRS to prioritize the highest risk workstations for timely

remediation. The SRAS will eventually replace the SCAP Compliance Checker tool currently in place at the IRS. See a diagram of the SRAS component in Appendix V.

- The Application Control Solution will allow the IRS to improve system integrity, security, and manageability by classifying known applications as either allowed or disallowed and thereby permit or prevent their execution.
- The Local Security Solution will provide centralized management of local administrative users and groups and allow the IRS to quickly and easily provision these accounts on the network. This component will resolve a current administrator password weakness that the IRS has identified and documented.

These components will allow the IRS to better monitor computer workstations on a more continuous basis, identify high-risk systems for immediate remediation, and provide some assurance that employee workstations are secure.

The Treasury Enhanced Security Initiatives Project Completed Key Documentation and Properly Acquired the Software

Key enterprise life cycle artifacts were properly completed

The TESI project team completed the key documentation required by the IRS's Enterprise Life Cycle development process. IRS IT organization project teams are required to follow the Enterprise Life Cycle development methodology. This approach is used to manage and implement business change through information systems initiatives and provides the artifacts and processes needed to accomplish business change in a consistent and repeatable manner. An important objective of the Enterprise Life Cycle is to enhance chances for success by reducing risk and ensuring compliance with internal and external standards and mandates.

An example of a key artifact that the TESI project properly completed is the System Deployment Plan. This plan defines the detailed set of activities required for the deployment of the TESI project components. We verified that the major sections of this plan were properly completed. The major sections are the site dependency matrix that provides the deployment activities and the corresponding responsible organizations, the roles and responsibilities section that identifies the roles and individuals responsible for deployment and testing activities at each site, and the site deployment schedule that provides a comprehensive list of the deployment activities with start and completion dates and durations.

Furthermore, the TESI project's Enterprise Life Cycle test plans are comprehensive and include the required details.

- The System Test Plan includes testing system controls surrounding the TESI project and includes policy checker and vulnerability scans.

- The End-of-Test Completion report indicates the project plans to document and follow through on test results.
- The Deployment Site Readiness Test plan indicates the project plans to conduct ongoing testing as the TESI project components are rolled-out to the various deployment sites.

The IRS was starting to test the TESI project components at the end of our fieldwork. However, our review of the TESI project test plans and early test results indicate the planned testing is more extensive than what is currently required by the IRS Cybersecurity function. Furthermore, the testing documentation is thorough and complete.

Stakeholders were involved in the design and development of the TESI project

The TESI Project Management team involved its key stakeholders in the design and development processes. The TESI project team held weekly meetings that included key stakeholders from the User and Network Services function, the Enterprise Services function, and the Enterprise System Management team in the Enterprise Operations function. These stakeholders provided comments on the Enterprise Life Cycle artifacts and documentation and informally communicated with the TESI project team frequently. This collaboration is important when deploying enterprise-wide software tools that require resource alignment and coordination between functions.

The TESI project software components were properly acquired

The IRS properly acquired the SRAS component of the TESI project from the General Services Administration's SmartBUY program, which pre-negotiates prices for the Federal Government in order to achieve maximum cost savings and the best quality for commodity software. The IRS also properly acquired the Local Security Solution and Application Control Solution components through the National Aeronautics and Space Administration Solutions for Enterprise-Wide Procurement contract. This contract also provides pre-competed discounted prices on information technology products for use by all Federal agencies. In addition, all three Phase 1 TESI project components were approved to be added to the IRS's Enterprise Standards Profile, which is the official list of information technology standards and approved software products at the IRS.

The SRAS component is SCAP-validated

We also determined that the SRAS component of the TESI project was validated by the NIST as a SCAP-compliant tool in accordance with the OMB's August 2008 mandate. This means the SRAS uses the standardized format and nomenclature by which security software products communicate software flaws and security configuration information. The SRAS utilizes the SCAP to organize, express, and measure security-related information in standardized ways, including unique identifiers for vulnerabilities. Furthermore, the SRAS was deployed

successfully at the U.S. Department of Health and Human Services, another large Federal agency with a geographically dispersed network.

The Treasury Enhanced Security Initiatives Project Experienced Several Delays

While the IRS completed and documented the Enterprise Life Cycle processes to develop the TESI project components, the project experienced several delays that affected its timely deployment.

Customer Account Data Engine, Version 2 – The Enterprise Operations function was responsible for ensuring the Customer Account Data Engine 2 system would operate as intended during the 2012 Filing Season. The mission of the Customer Account Data Engine 2 Program is to provide state-of-the-art individual taxpayer account processing and technologies to improve service to taxpayers and enhance tax administration. Once complete, the new modernized environment should allow the IRS to more effectively and efficiently update taxpayer accounts, support account settlement and maintenance, and process refunds on a daily basis. This high-profile modernization project was the top information technology priority for the IRS and consumed significant resources in the Enterprise Operations function in Calendar Years 2011 and 2012. Several information technology projects at the IRS were affected, including the TESI project, because the projects depend on the Enterprise Operations function to establish foundational infrastructure, such as the Symantec Management Platform discussed in detail below.

Symantec Infrastructure Upgrade – As the IRS prepared to upgrade its infrastructure from Altiris 6.9 to Symantec Management Platform version 7.0 in April 2011, officials from the Symantec Corporation notified the IRS that version 7.0 had several problems that required resolution before the IRS could deploy the upgrade on its network. The IRS had to delay this infrastructure upgrade until the Symantec Corporation released its Symantec Management Platform version 7.1, which the IRS approved for deployment in May 2011. However, as of August 2012, 16 months after the planned upgrade, the IRS has not successfully deployed and stabilized version 7.1.

At the end of Calendar Year 2011, Enterprise Operations function officials began working with contractors from the Symantec Corporation on a daily basis to resolve the Symantec Management Platform version 7.1 performance issues. Symantec and Enterprise Operations function officials determined on January 5, 2012, that the Symantec Management Platform was not operating as intended because the IRS's virtualized server environment could not provide the required input/output speeds that are necessary for the Symantec Management Platform to function properly. Symantec Corporation reiterated the required resources for the platform and recommended physical structured query language servers be used instead of virtualized servers.

The Enterprise Operations function agreed with the recommendation but has not installed the physical servers as of August 2012.

Filing Season Moratoriums – The IRS establishes a filing season moratorium each year to stabilize its information technology production environment during peak tax return processing times. During the moratorium, no changes to the information technology environment are allowed to be implemented without executive approval. The TESI project experienced delays due to two separate filing season moratoriums in effect from November 30, 2010, through May 23, 2011, and from November 1, 2011, through May 21, 2012.

The cumulative effect of these delays resulted in the IRS acquiring software licenses for each component of the TESI project that have not yet been implemented. As of August 2012, the IRS has paid $687,180 for license renewal and maintenance fees that expire in September 2012 for products that are not yet deployed.

The Cybersecurity and Privacy Governance Board Did Not Take Required Actions to Manage Project Delays

The Cybersecurity and Privacy Governance Board held its first meeting in November 2009 with a charter to resolve project issues; manage cost, schedule, and scope variances; and escalate any unresolved issues to the higher level Security Services and Privacy Executive Steering Committee. However, this Board did not take these actions to address the delays that the TESI project encountered.

In March 2011, the TESI project first reported to the Cybersecurity and Privacy Governance Board that significant delays were hindering the project from deploying on time, and the project needed a new baseline. Specifically, the delay in upgrading the Symantec Management Platform, which we explained earlier in this report, was reported. The same delay was then reported to the Board on a regular basis for the next 16 months, through July 2012, but the Board did not take actions to manage the costs associated with the delay or approve a new baseline for the project until the July 2012 meeting. Considering the TESI project was originally scheduled to deploy the SRAS in December 2010, the project continued to operate for 19 months without an approved baseline, from December 2010 to July 2012. Additionally, at no point did the Board request the TESI project to report its total life cycle costs. This action would have allowed the Board to analyze cost variances against the original planned cost at the start of the project and the actual and revised estimated costs. Finally, the Board did not escalate the significant delays to the higher level Executive Steering Committee.

The Cybersecurity and Privacy Governance Board Chair informed us that the Board did not consider postponing the project to conserve funds for other information technology projects. The Board mistakenly assumed that the Enterprise Operations function would provide the support that the TESI project needed in the following month. However, at the end of our fieldwork, in August 2012, the Enterprise Operations function still had not installed the physical servers or

stabilized the Symantec Management Platform infrastructure. Furthermore, the IRS paid contractors $1,151,939 for TESI project support from December 2010, the original SRAS deployment date, through April 2012.[6] The TESI project currently plans to deploy its Phase 1 components in May 2013.

Recommendations

The Chief Technology Officer should direct the Cybersecurity and Privacy Governance Board to:

Recommendation 1: Review total actual life cycle costs for projects at least quarterly and review variances between actual costs and the originally proposed estimated costs.

> ***Management's Response:*** The IRS agreed with this recommendation. The Cybersecurity and Privacy Governance Board will review total actual life cycle costs for projects at least quarterly and review variances between actual costs and estimated costs.

Recommendation 2: Manage costs by considering the postponement of projects with long-term delays.

> ***Management's Response:*** The IRS agreed with this recommendation. The Cybersecurity and Privacy Governance Board will consider postponing projects with long-term delays and will present its recommendation for postponement to the higher level governance board, the Security Services and Privacy Executive Steering Committee, for concurrence.

Recommendation 3: Escalate ongoing project delays to the Security Services and Privacy Executive Steering Committee, as required by its charter.

> ***Management's Response:*** The IRS agreed with this recommendation. The Cybersecurity and Privacy Governance Board will escalate ongoing delays that cannot be resolved to the higher level governance board, the Security Services and Privacy Executive Steering Committee, for resolution.

[6] See Appendix IV for more details.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether the IRS is effectively and efficiently implementing its continuous monitoring tool to monitor security settings on employee workstations and laptop computers. To accomplish our objective, we:

I. Evaluated the continuous monitoring capability that is currently in place for workstations and determined whether the SRAS[1] will provide the OMB-mandated functionality once implemented.

   A. Reviewed the performance and functionality of the Space and Naval Warfare Systems Command's SCAP Compliance Checker tool currently in place at the IRS to identify weaknesses in the tool, and confirmed that the NIST approved it to be SCAP-compliant.

   B. Determined whether the SRAS system will provide the OMB-mandated functionality for scanning and monitoring security configurations, once deployed, and determined whether the tool is NIST-validated.

II. Determined whether the IRS properly and efficiently procured a SCAP-validated workstation configuration monitoring tool.

   A. Determined whether the SRAS component and any related contract support services met the requirements for the General Services Administration's SmartBUY program and other Federal purchasing programs by obtaining and analyzing acquisition documentation and program requirements.

   B. Interviewed the appropriate contracting officer and TESI project management to obtain explanations of the acquisition processes that were followed.

   C. Determined whether premature acquisition of tools, licenses, infrastructure, or services resulted in wasted funds.

III. Determined whether the IRS has effectively managed the TESI project to implement the SRAS within its budget and schedule.

   A. Determined whether the TESI project was properly classified as a nonmajor acquisition per relevant regulations.

[1] See Appendix VI for a glossary of terms.

B. Determined whether the TESI project followed the correct Enterprise Life Cycle path; properly and timely completed key Enterprise Life Cycle deliverables, artifacts, and processes; ensured that major stakeholders were actively involved throughout the project development phases, especially during critical review processes such as Customer Technical Reviews, Life Cycle Stage reviews, and Milestone Readiness reviews; and timely and properly conducted Milestone Readiness Reviews and Milestone Exit Reviews, which are mandatory for all projects.

C. Identified the deadlines for implementing the SRAS and evaluated the TESI project's success in meeting the deadlines. We also determined whether the IRS rebaselined the TESI project in accordance with OMB guidance and determined the number of times the project was officially rebaselined.

D. Determined the cause and effect of the delays the IRS experienced in implementing the SRAS. We interviewed TESI project management, Enterprise Operations function officials, and the Chair of the Cybersecurity and Privacy Governance Board to quantify delays and their causes. We reviewed Board meeting minutes to determine whether the delays, along with the cause and effect, were timely reported to the Board, and evaluated the Board's actions to address the delays.

E. Determined the overall TESI project costs to date and estimated costs remaining for implementation.

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 the following internal controls were relevant to our audit objective: the OMB, the NIST, and related IRS guidelines for continuous monitoring of security configurations on computer workstations and the IRS's efforts to implement these controls in order to protect the IRS network and data. We evaluated these controls by conducting interviews and meetings with TESI project management and security staff at the IRS responsible for addressing noncompliant workstations. We also reviewed software and contractor support acquisitions for the TESI project, as well as related IRS processes and regulatory requirements information.

Appendix II

Major Contributors to This Report

Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Director
W. Allen Gray, Audit Manager
Jena R. Whitley, Lead Auditor
Charles O. Ekunwe, Senior Auditor
Mary L. Jankowski, Senior Auditor
Linda L. 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
Deputy Commissioner for Services and Enforcement SE
Associate Chief Information Officer, Cybersecurity OS:CTO:C
Associate Chief Information Officer, Enterprise Operations OS:CTO:EO
Associate Chief Information Officer, Strategy and Planning OS:CTO:SP
Associate Chief Information Officer, User and Network Services OS:CTO:UNS
Director, Office of Research, Analysis, and Statistics RAS
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

Outcome Measure

This appendix presents detailed information on the measurable impact that our recommended corrective actions will have on tax administration. This benefit will be incorporated into our Semiannual Report to Congress.

Type and Value of Outcome Measure:

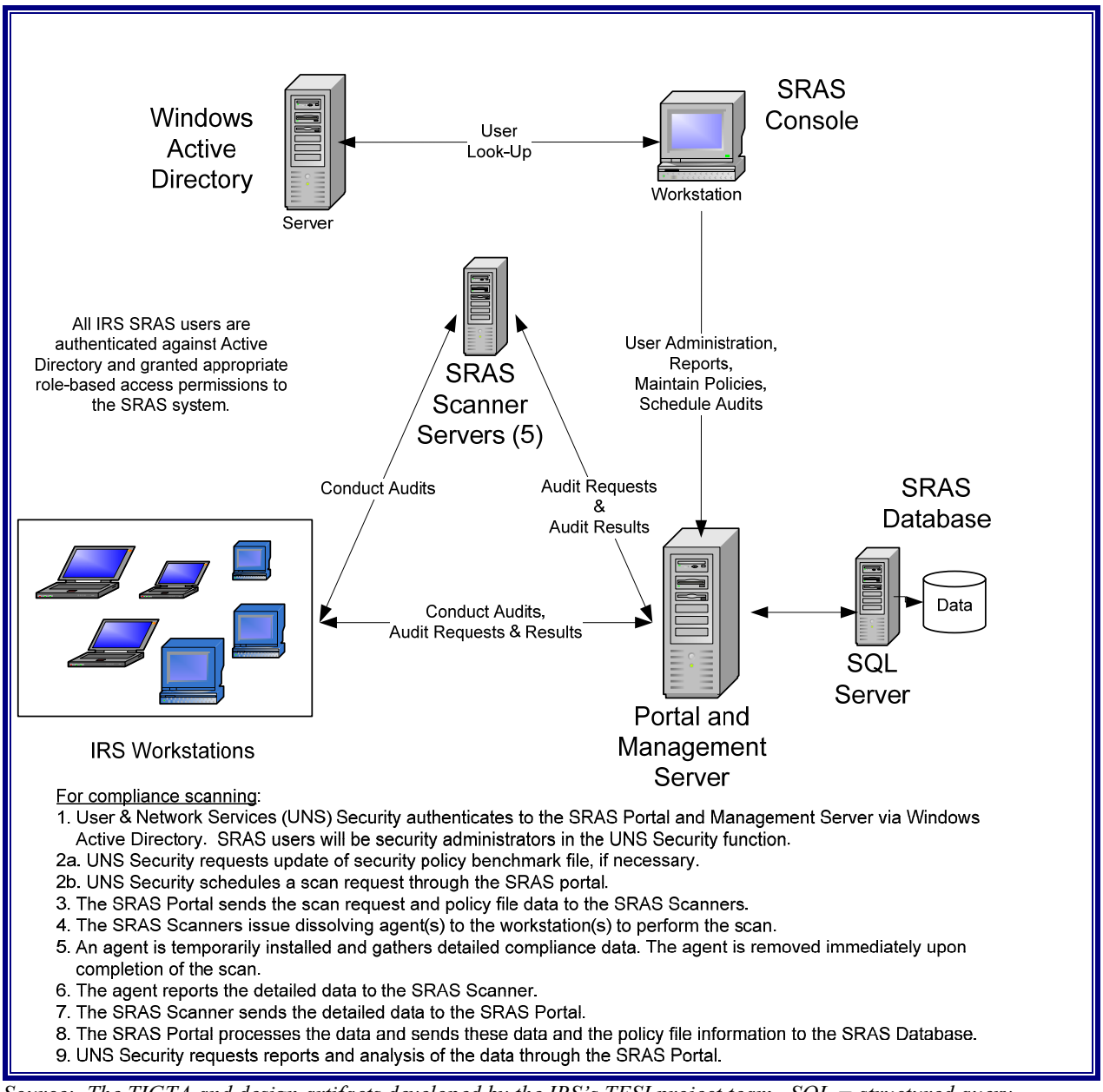
- Inefficient Use of Resources – Potential; $1,151,939 in contractor support services (see page 7).

Methodology Used to Measure the Reported Benefit:

The IRS spent $1,151,939 on contractor support services for the TESI project from its original December 2010 planned deployment of the SRAS component through April 2012. The TIGTA's recommendation to the Cybersecurity and Privacy Governance Board to manage project costs and consider postponing projects with long-term delays will enable the IRS to improve its process to more efficiently manage information technology project resources.

Appendix V

Symantec Risk Automation Suite Diagram



Source: The TIGTA and design artifacts developed by the IRS's TESI project team. SQL = structured query language.

Appendix VI

Glossary of Terms

Term	Definition
Acquisition	The process of obtaining products or services through contractual agreements with outside vendors or contractors.
Altiris	Company acquired by Symantec Corporation in 2007.
Application	An information technology component of a system that utilizes information technology resources to store, process, retrieve, or transmit data or information using information technology hardware and software.
Artifact	The tangible result (output) of an activity or task performed by a project during the Enterprise Life Cycle.
Baseline	A benchmark that includes project costs, schedule, and scope against which project performance is measured.
Contractor	An organization external to the IRS that supplies goods and services according to a formal contract. A contractor is a type of provider.
Cyber	Cyber is often used for "electronic" or "computer-related."
Dissolving Agent	A computer program that is used for collecting data locally at endpoints without requiring communication back to the scanner; once data are collected, the agent sends the data back to the scanner and deletes itself from the endpoint.
Enterprise	An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management, human resources, security, information systems, and mission management.

Term	Definition
Enterprise Life Cycle	The Enterprise Life Cycle is the approach used by the IRS to manage and implement business change through information systems initiatives. The Enterprise Life Cycle provides the direction, processes, tools, and assets necessary to accomplish business change in a consistent and repeatable manner.
Federal Desktop Core Configuration	Designed to provide a single standard, enterprise-wide managed environment for desktops and laptops by using a common configuration to improve security and reduce costs.
Governance	The exercise of external control over a project or program by personnel or organizations that are not part of or directly associated with the team performing the work on a day-to-day basis.
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.
Malware (also Malicious Code)	Software or firmware intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.
Modernization	Modernization is the process of updating, improving, and bringing in line with modern standards. Modernization is an IRS program that includes Organization Modernization and Business System Modernization (processes and technology).

Term	Definition
National Institute of Standards and Technology	The NIST, under the Department of Commerce, is responsible for developing standards and guidelines for providing adequate information security for all Federal Government agency operations and assets.
Network	Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.
Nonmajor Project	A project that meets OMB criteria for nonmajor projects.
Office of Management and Budget	Implementation and enforcement arm of Presidential policy Government-wide that carries out its mission through budget development and execution; oversight of agency performance, Federal procurement, and financial management; and the review of, among other things, all significant Federal regulations by executive agencies.
Project	A group of tasks to accomplish a specific objective, with a beginning and ending date, that is planned, monitored, and measured; follows a life cycle process; and results in deliverables or end products.
Release	A collection (one or more) of changes made since the last deployment of a system. A release can also refer to an initial deployment of software or hardware and may or may not be used in the context of one or more projects.
Remediation	The act of correcting a vulnerability or eliminating a threat through activities such as installing a patch, adjusting configuration settings, or uninstalling a software application.
Risk	The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
Security Content Automation Protocol	A method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation.

Term	Definition
Server	A physical computer (a computer hardware system) dedicated to running one or more services (as a host), to serve the needs of the users of other computers on the network. Depending on the computing service that it offers, it could be a database server, file server, mail server, print server, web server, gaming server, or some other kind of server.
Structured Query Language	A special-purpose programming language designed for managing data in relational database management systems.
Symantec Management Platform	Provides a set of services that information technology-related solutions can leverage. Because solutions share the same platform, they can share platform services as well as data. This close integration of solutions and the platform makes it easier to use the different solutions because they work in a common environment and are administered through a common interface. Components include role-based security; client communications and management; event-triggered and scheduled task and policy execution; file deployment and installation; reporting; and centralized management through a single, common interface.
Symantec Risk Automation Suite	Tool with capabilities that relate directly to the objectives of the NIST SCAP, a method for using specific standards to enable automated and integrated vulnerability management and measurement, and policy compliance evaluation. Provides continuous and automated information technology risk metrics.
System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. A system normally includes hardware, software, information, data, applications, communications, and people.

Term	Definition
Threat	Any circumstance or event with the potential to adversely affect organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, or denial of service. Also, the potential for a threat source to successfully exploit an information system's vulnerability.
User	Individual, or (system) process acting on behalf of an individual, authorized to access an information system.
Virtualized Server	Running applications in separate, isolated partitions (separate "virtual machines") within a single server. Widely used in enterprise and cloud computing data centers, each virtual machine runs its own operating system and application and can be moved or copied from one server to another for load balancing or to expand processing capability.
Virus	A piece of programming code usually disguised as something else that causes some unexpected and, for the victim, usually undesirable event and which is often designed so it is automatically spread to other computers.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Vulnerability Scan	The process of proactively identifying vulnerabilities of an information system in order to determine if and where a system can be exploited or threatened. Employs software that seeks out security flaws based on a database of known flaws, tests systems for the occurrence of these flaws, and generates a report of the findings that an individual or an enterprise can use to tighten the network's security.

Appendix VII

Management's Response to the Draft Report

CHIEF TECHNOLOGY OFFICER

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

DEC 20 2012

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Terence V. Milholland
Chief Technology Officer

SUBJECT: Draft Audit Report–Significant Delays Hindered Efforts to Provide Continuous Monitoring of Security Settings on Computer Workstations (Audit # 201220008) (e-trak # 2013-37567)

Thank you for the opportunity to review and respond to the subject audit report. We appreciate that your report acknowledged that the Internal Revenue Service:

- Used a Secure Content Automation Protocol (SCAP) Compliance Checker Tool to scan Federal Desktop Core Configuration settings on employee workstations and laptops, and the tool is SCAP-compliant as required by the Office of Management and Budget.
- Initiated the Treasury Enhanced Security Initiatives (TESI) project to replace the current compliance tool with more robust technology.
- Completed and documented Enterprise Life Cycle process requirements to develop the TESI project components.

The security and privacy of taxpayer information is of utmost importance to us, and your report recommendations will further assist us in continuing to improve our information technology security posture. We agree with the three report recommendations. The attachment to this memo details our planned corrective actions to implement the recommendations.

We value your continued support and the assistance and guidance your organization provides. If you have any questions, please contact me at (202) 622-6800 or David W. Stender, Associate Chief Information Officer for Cybersecurity, at (202) 622-8910.

Attachment

Draft Audit Report – Significant Delays Hindered Efforts to Provide Continuous Monitoring of Security Settings on Computer Workstations (Audit # 201220008; e-trak # 2013-37567)

RECOMMENDATION #1: The Chief Technology Officer should direct the Cybersecurity and Privacy Governance Board to review total actual life cycle costs for projects at least quarterly and review variances between actual costs and the originally proposed estimated costs.

CORRECTIVE ACTION #1: The IRS agrees with the recommendation. The Cybersecurity Privacy and Governance Board will review total actual life cycle costs for projects at least quarterly and review variances between actual costs and the originally proposed estimated costs.

IMPLEMENTATION DATE: June 1, 2013

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 direct the Cybersecurity and Privacy Governance Board to manage costs by considering the postponement of projects with long-term delays.

CORRECTIVE ACTION #2: The IRS agrees with the recommendation. The Cybersecurity and Privacy Governance Board will consider postponements of projects with long-term delays and will present the recommendation to the higher-level governance board, the Security Services and Privacy Executive Steering Committee, for concurrence.

IMPLEMENTATION DATE: June 1, 2013

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 #3: The Chief Technology Officer should direct the Cybersecurity and Privacy Governance Board to escalate ongoing project delays to the Security Services and Privacy Executive Steering Committee, as required by its charter.

Draft Audit Report – Significant Delays Hindered Efforts to Provide Continuous Monitoring of Security Settings on Computer Workstations (Audit # 201220008; e-trak # 2013-37567)

CORRECTIVE ACTION #3: The IRS agrees with the recommendation. The Cybersecurity and Privacy Governance Board will escalate ongoing delays that cannot be resolved to the higher-level governance board, the Security Services and Privacy Executive Steering Committee, for resolution.

IMPLEMENTATION DATE: June 1, 2013

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.