*TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION*

# *Progress Has Been Slow in Implementing Federal Security Configurations on Employee Computers*

**March 27, 2009**

**Reference Number: 2009-20-055**

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*
*Email Address | inquiries@tigta.treas.gov*
*Web Site | http://www.tigta.gov*

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

March 27, 2009

**MEMORANDUM FOR** CHIEF TECHNOLOGY OFFICER

Michael R. Phillips

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

**SUBJECT:** Final Audit Report – Progress Has Been Slow in Implementing Federal Security Configurations on Employee Computers (Audit # 200820026)

This report presents the results of our review to determine whether the Internal Revenue Service (IRS) has made adequate progress in implementing required Federal secure configurations on employee computers. This audit was included in the Treasury Inspector General for Tax Administration Fiscal Year 2008 Annual Audit Plan and is part of our statutory requirement to annually review the adequacy and security of IRS technology.

## *Impact on the Taxpayer*

IRS employees use desktop and laptop computers to perform their tax administration duties. Because taxpayers expect the IRS to protect their privacy and personal information, the security of employee computers is critical. The IRS is attempting to adopt a standard set of Federally required computer configuration settings and procedures to improve security and reduce operating costs. Although the IRS has taken actions, implementation of the configuration settings has been slow and some of the requirements have not been implemented. Without a complete set of security configuration settings, the IRS is at risk of business disruption or unauthorized access to taxpayers' personal information.

## *Synopsis*

The Office of Management and Budget (OMB) required Federal Government agencies that use the Windows XP or VISTA[1] operating systems to adopt a standard set of configuration settings

[1] Windows XP and VISTA are computer operating systems produced by the Microsoft Corporation for use on desktop and laptop computers.

by February 1, 2008. These configuration settings are referred to as the Federal Desktop Core Configuration (FDCC). The intent of the requirement was to improve security and reduce operating costs.

The IRS faces many challenges in implementing the FDCC. IRS employees use more than 98,000 desktop and laptop computers located in approximately 670 facilities throughout the nation and operate more than 1,900 software applications, of which approximately 300 were internally developed for specific IRS business processes. As part of the implementation effort, the IRS must test each application to ensure it operates properly with the FDCC.

The IRS has made slow progress in implementing the FDCC settings. On October 29, 2008, the IRS implemented 102 settings on IRS workstations. However, these FDCC settings were installed on employee computers 9 months after the deadline set by the OMB for agencies to complete their FDCC implementation efforts. As of December 11, 2008, the IRS had implemented 205 (81 percent) of the 254 FDCC settings.

The delay in implementing the FDCC was primarily due to the untimely creation of a project team responsible for the FDCC implementation. The OMB issued the FDCC directive in March 2007. However, the IRS did not establish a project team until January 2008, 10 months after the OMB issued the directive and 1 week before the deadline for completing the FDCC implementation. The untimely creation of the project team occurred because some IRS officials mistakenly assumed the IRS' current common operating environment[2] was compliant with the FDCC.

We also found that, once the project team was established, the project leaders did not follow some basic project management practices while testing software applications for FDCC compatibility. The master control list used by the project leaders was incomplete and did not account for many applications that needed to be tested. The discovery of 92 applications after the 2-week testing phase required project leaders to initiate additional testing. In addition, the Work Breakdown Structure[3] developed for the project lacked critical tasks that were needed to accomplish the project's objectives. When basic project management practices are not followed, the risk of business disruption increases. As an illustration, when the IRS implemented its first set of FDCC settings, one critical application, which was not tested, began experiencing problems and could have had severe consequences if the IRS had been unable to reverse the settings.

[2] To ensure consistency across the IRS network and improve security, the IRS created the common operating environment, which is a standardized set of commercial off-the-shelf and internally developed applications to support the needs of all IRS employees using Microsoft Windows. The common operating environment also allows the IRS to control security configuration settings and software on its workstations by changing one master template and then installing it on all computer workstations throughout the agency.

[3] A deliverable-oriented grouping of project elements that organizes and defines the total scope of the project.

The IRS also has not implemented some of the OMB's other FDCC mandates. An automated monitoring tool to detect and monitor changes to the FDCC settings after they are installed on employees' workstations has not been implemented. In addition, the IRS has not modified its software contracts to ensure software acquisitions operate properly with the FDCC settings. We identified 27 of 30 contracts for new software products that did not include the required FDCC contract language.

## Recommendations

To ensure that basic project management practices are followed and OMB mandates are implemented, the Chief Technology Officer should 1) provide training to the FDCC project managers to ensure their project management skills and qualifications are sufficient, 2) instruct the project leaders to develop and maintain an accurate control list of applications that require testing, 3) conduct an analysis and consider the feasibility of acquiring a monitoring tool from the General Services Administration's blanket purchase agreement, and 4) direct the Cybersecurity office to coordinate with the Procurement Division and prioritize the work necessary to include the required FDCC contract language in information technology acquisitions.

## Response

IRS management agreed with the recommendations. The IRS will provide project management training for the FDCC project managers and ensure the master control list of applications is maintained and updated. The Chief Technology Officer will conduct a cost-benefit analysis to determine whether the purchase of a separate monitoring tool from the General Services Administration's SmartBuy Program is in the IRS' best interest. Finally, the IRS plans to issue an agency-wide policy and interim acquisition procedures that will incorporate the FDCC contract language in information technology acquisitions. Management's complete response to the draft report is included as Appendix IV.

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

# *Table of Contents*

**Appendices**

# *Abbreviations*

| | |
|---|---|
| FDCC | Federal Desktop Core Configuration |
| IRS | Internal Revenue Service |
| OMB | Office of Management and Budget |

# Background

Internal Revenue Service (IRS) employees use desktop and laptop computers to perform their tax administration duties. Because taxpayers expect the IRS to protect their privacy and personal information, the security of employee computers is critical. Without a complete set of security configuration settings for employee workstations, the IRS is at risk of business disruption or unauthorized access to taxpayers' personal information.

In March 2007, the Office of Management and Budget (OMB) required[1] Federal Government agencies that use the Windows XP or VISTA[2] computer operating systems to adopt a standard set of configuration settings. The intent of the requirement was to improve security and reduce operating costs. The configuration settings were developed by the National Institute of Standards and Technology,[3] the Department of Defense, and the Department of Homeland Security and are referred to as the Federal Desktop Core Configuration (FDCC). The OMB required that all agencies adopt the FDCC by February 1, 2008. The National Institute of Standards and Technology published the first set of FDCC settings in July 2007. This first set included 229 mandatory security settings and an additional 329 configuration settings that are recommended to improve security and reduce risks and costs associated with software vulnerabilities.

In addition to implementing the FDCC settings, the OMB required[4] agencies to ensure that software acquisitions operate properly with the FDCC settings. Agencies are required to incorporate specific language in solicitations for new software and require vendors to certify that their products operate effectively using the configurations. The Federal Acquisition Regulation[5] was also revised to require agencies to include the FDCC requirement in contracts.

The IRS faces many challenges in implementing the FDCC settings. IRS employees use more than 98,000 desktop and laptop computers located in approximately 670 facilities throughout the

[1] OMB Memorandum M-07-11, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*, dated March 22, 2007.
[2] Windows XP and VISTA are computer operating systems produced by the Microsoft Corporation for use on desktop and laptop computers.
[3] The National Institute of Standards and Technology, 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.
[4] OMB Memorandum M-07-18, *Ensuring New Acquisitions Include Common Security Configurations*, dated June 1, 2007.
[5] The Federal Acquisition Regulation is the principal set of rules in the Federal Acquisition Regulations System. This System consists of regulations issued by Federal Government agencies to govern the "acquisition process," which is the process through which the Federal Government purchases goods and services.

nation and operate more than 1,900 software applications, of which approximately 300 were internally developed for specific IRS business processes. As part of the implementation effort, the IRS must test each application to ensure the applications operate properly with the FDCC settings.

Other Federal Government agencies have also encountered significant challenges in implementing the FDCC. During a January 2008 conference with the OMB, one agency representative stated that the FDCC settings would "break their systems." Another agency representative made similar remarks by stating that it would not be compliant with the FDCC because a number of the settings caused problems on their computer systems.

After installing the FDCC on desktop and laptop computers, the IRS also faces challenges regarding how to maintain the settings because system administrators throughout the IRS have the ability to change the settings on employee computers. To address these challenges, the OMB and the Department of the Treasury directed[6] the IRS to implement an automated tool to check that security configurations are continually maintained on computer workstations.

We focused our review on the FDCC settings that were tested and installed by the IRS project team led by officials in the Modernization and Information Technology Services Division's Cybersecurity office and the End User Equipment and Services organization, which manages more than 91 percent of the desktop and laptop computers used by the IRS. This review was performed in the Modernization and Information Technology Services Division office in New Carrollton, Maryland; the Martinsburg Computing Center in Martinsburg, West Virginia; and the IRS Procurement offices in Oxon Hill, Maryland, during the period June through December 2008. 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.

[6] Treasury Memorandum TCIO M 08-01, *Enhanced Cyber Security Controls*, dated December 20, 2007.

# Results of Review

While the IRS has taken some actions to implement the FDCC, the progress has been slow and some of the security settings have not yet been implemented. The primary reason for the slow progress was due to the IRS not timely creating a project team to implement the FDCC. Once established, the project team did not follow basic project management practices. In addition, the IRS has not implemented an automated tool to detect and monitor changes to the FDCC settings after they are implemented on IRS workstations, and it did not revise the language in its software contracts to ensure new software products operate properly with the FDCC.

## Actions Have Been Taken to Implement the Federal Desktop Core Configuration Settings

The IRS has taken actions to implement some of the FDCC settings. Specifically:

- The IRS updated its internal procedures to include the FDCC settings applicable to the Windows XP operating system.
- The IRS selected 50 other settings, in addition to the 229 mandated security settings recommended by the National Institute for Standards and Technology, to implement in the IRS common operating environment.[7]
- The IRS had implemented 103 (41 percent) of the 254[8] FDCC settings in its common operating environment prior to the start of the FDCC project. This effort provided a solid foundation to start the implementation activities.
- The project team improved its test methodology after consulting with the Microsoft Corporation. The new test methodology allowed the IRS to test applications in the users' work environments with employees from each business operating division. The testers were assigned to support the FDCC effort due to their knowledge of the applications. This approach allowed the project team to gain support from the business units and increase the number of testers.

[7] To ensure consistency across the IRS network and improve security, the IRS created the common operating environment, which is a standardized set of commercial off-the-shelf and internally developed applications to support the needs of all IRS employees using Microsoft Windows. The common operating environment also allows the IRS to control security configuration settings and software on its workstations by changing one master template and then installing it on all computer workstations throughout the agency.
[8] Because 25 of the 229 settings relate to the VISTA operating system, which the IRS does not operate, the actual number of FDCC settings the IRS plans to implement is 254 (229 + 50 – 25 = 254).

- On October 29, 2008, the IRS implemented 102 FDCC settings. Combining this effort with the settings already implemented on its common operating environment, the IRS implemented 205 (81 percent) of the 254 settings required on IRS workstation and laptop computers. However, this progress occurred 9 months after the OMB deadline and, as of December 11, 2008, several of the 229 mandatory settings were still not implemented.

***Management Actions*****:** Subsequent to the completion of our fieldwork, the IRS advised us that it implemented 13 additional FDCC settings on IRS workstations and laptop computers. In addition, the IRS classified eight settings as corporate deviations, which indicates the setting cannot be implemented because doing so would adversely impact an application.

## A Project Team Was Not Established in a Timely Manner to Effectively Comply With the Office of Management and Budget Deadline

Despite the actions previously discussed, overall efforts toward implementing FDCC settings on IRS computers have been slow. The IRS Modernization and Information Technology Services Division should have established an FDCC project team to assess the scope of work that was needed to implement the FDCC in a timely manner soon after the OMB issued its FDCC directive in March 2007. However, the IRS waited until January 2008, 10 months after the OMB memorandum was issued and 1 week before the February 1, 2008, OMB deadline established for implementing the FDCC.

In October 2007, the Associate Chief Information Officer, Cybersecurity, sent an email to IRS executives advising them to consider the implications of the OMB requirement. However, actions to establish a team were not taken timely because some IRS officials assumed the existing common operating environment was compliant with the FDCC requirements. The IRS End User Equipment and Services organization did not learn of the OMB requirement until October 2007, at which time it discussed the requirement with the Microsoft Corporation. During this meeting, the magnitude and complexity of implementing the FDCC settings was realized. However, the IRS waited an additional 3 months before appointing a project leader.

The delay in establishing a project team was the primary reason the IRS was untimely in complying with the FDCC requirement, possibly resulting in inadequate security over taxpayer data and computer operations. However, we did not assess the effect of the untimely implementation and did not identify any security breaches as a result of untimely and incomplete implementation of FDCC settings on IRS computers.

## Some Basic Project Management Practices Were Not Followed

In addition to the delay in assembling a project team to lead the FDCC implementation efforts, the IRS did not follow some basic project management practices. Project management is the application of knowledge, skills, tools, and techniques to project activities to ensure a project meets its goals. In general, project management can be broken down into the processes of planning, executing, monitoring, controlling, and closing a project. The project manager is the person responsible for accomplishing the project objectives.

The *Guide to the Project Management Body of Knowledge*[9] states that the project manager should maintain an accurate and timely information base. Continuous monitoring provides insight into the health of a project and identifies areas that require special attention. The project manager should maintain a complete master control list of applications throughout the test phase to monitor and control the testing. This basic project management practice allows the project leader to ensure that all applications identified in the planning phase are actually tested and that the test results are monitored for each application. The project manager should also develop and maintain a Work Breakdown Structure[10] to plan and manage the tasks necessary to accomplish the project's objectives.

## Inadequate controls resulted in some applications not being tested

The FDCC project leaders tested IRS applications to ensure that they would properly operate with the FDCC settings. However, they did not control and account for all applications that needed to be tested. The master control list of applications used by the project leaders was incomplete and did not account for many applications. In addition, the project leaders did not update the master control list with test results to monitor the testing for each application and ensure that all applications were tested.

The project leaders coordinated with the Modernization and Information Technology Services Division's Applications Development organization after completing a 2-week testing exercise on September 16, 2008, and discovered 92 applications that were not accounted for on the master control list. The discovery of the 92 applications required the project leaders to conduct additional testing to ensure the applications would properly operate with the FDCC settings.

Examples of omitted applications included the:

- **Electronic Installment Agreement Project.** This application offers taxpayers the ability to establish streamlined payment agreements over the Internet. It allows taxpayers or authorized representatives (Power of Attorney) to self-qualify, apply for an installment agreement, and receive online approval notification.

- **Enterprise Logistics Information Technology.** This application is an integrated, web-based, real-time supply chain execution system used by the Accounts Management and Compliance Services Processing organizations to receive, store, manage, and distribute IRS tax forms.

[9] Published in 2004 by the Project Management Institute, it is an internationally recognized standard that provides the fundamentals of project management as they apply to a wide range of projects, including software development.
[10] A deliverable-oriented grouping of project elements that organizes and defines the total scope of the project.

The project leaders also did not use sources available to them to complete their master control list of applications. The list was developed based on applications submitted by volunteer testers and applications designated as important by IRS business units. However, other sources were available such as the list of applications the IRS reports to the OMB as part of the annual Federal Information Security Management Act[11] compliance reporting process. This list contained 29 applications that were not accounted for on the project leaders' master control list. When we provided the names of the 29 applications to the project leaders, they delayed the implementation of the FDCC settings to ensure the applications were tested. They found that 8 applications had not been tested and 21 applications were tested but were not accounted for on the master control list. Examples of missing applications from this source included the:

- **Integrated Collection System.** This application provides workload management, case assignment/tracking, inventory control, electronic mail, and case analysis tools to support the Small Business/Self-Employed Division collection fieldwork.
- **Tip Database.** This application is used by the Small Business/Self-Employed Division to store all tip rate agreement data for casinos. The Tip Database helps to quickly and more accurately identify nonfilers or tip income underreporters by eliminating errors from a previously manual process.

Another source available to the project leaders was the inventory of new applications maintained by the Workstation Standards office, which is part of the End User and Equipment Services organization within the Modernization and Information Technology Services Division. We determined that five applications, acquired between January 22 and October 10, 2008, were installed in the IRS operating environment without being tested for compatibility with the FDCC settings. The project leaders believed the Workstations Standards office was responsible for testing new software applications against the FDCC settings. However, the Workstation Standards office tested the new applications for compatibility with the IRS' current common operating environment image, which did not include the new FDCC settings.

In addition to not maintaining a complete master control list of applications, the project leaders did not account for the applications' test results on the master control list. The test results for each application should have been accounted for and recorded on the master control list to monitor test results and ensure each application was tested. The project leaders relied on the volunteer testers to test the applications that they use in their normal workday and to prepare a helpdesk ticket if they found a problem. The testers were also asked to record their test results on spreadsheets. However, the results from the testers' spreadsheets were not recorded on the master control list to ensure that all applications were tested.

[11] The Federal Information Security Management Act is part of the E-Government Act of 2002, Pub. L. No. 107-347, Title III, 116 Stat. 2946 (2002).

The risk of business disruption increases when the control and monitoring over testing are inadequate. This risk was realized after the project team installed the first group of FDCC settings on October 29, 2008. Within a few days, the Financial Management Secure Payment System, a critical application, began to experience problems. The application, which is used to certify tax refunds, was not tested. The IRS must pay significant penalties when it is unable to timely certify refund checks. In this instance, the IRS avoided paying penalties because the project team was able to reverse the FDCC settings from the computers of employees who use the application. However, the incident highlights the risk of not maintaining a complete master control list of applications and ensuring that all applications are tested.

***A critical application used to certify tax refunds began to experience major problems after the IRS installed the first group of FDCC settings.***

## *The Work Breakdown Structure was inadequate to plan and manage the FDCC project*

The Work Breakdown Structure developed by the project leaders lacked critical tasks that were needed to accomplish the project's objectives. Examples of the tasks include:

- Conduct a gap analysis to identify missing applications.
- Develop and maintain a master control inventory of applications and test results.
- Develop a "roll-back" plan in the event that a need arises to reverse the FDCC settings from IRS workstations.
- Develop presentations and present status report briefings to stakeholders and oversight agencies such as IRS executives, the OMB, the Department of the Treasury, and the Treasury Inspector General for Tax Administration.
- Coordinate with the IRS project that is planning to replace all IRS laptop and desktop computers.

Some of the critical work and activities were included in the Work Breakdown Structure. However, the work and activities were described at a high level. Several activities lacked detailed descriptions and delineation. The Project Management Institute defines a Work Breakdown Structure as a deliverable-oriented hierarchical decomposition of the work to be executed by the project team to accomplish the objectives and create the required deliverables.[12] Each descending level represents an increasingly detailed definition of the project work.

[12] The Project Management Institute book entitled *Practice Standard for Work Breakdown Structures*, Second Edition, 2006, provides guidance on the creation of a Work Breakdown Structure.

The Work Breakdown Structure also lacked a critical path, which is the sequence of activities that must be completed on schedule for the entire project to be completed on schedule. A critical path allows the project manager to identify and calculate the effect of delays and manage the inevitable challenges that occur on all large complex projects.

A Work Breakdown Structure that does not include the planned work, critical path, and detailed descriptions of activities does not fulfill its primary purpose, which is to help the project leader manage the project, identify schedule delays, and ensure completion of all tasks in a timely manner. Considering the complexity of implementing FDCC settings throughout the IRS, we believe a more complete Work Breakdown Structure could have improved the planning and the timeliness of implementing the FDCC settings.

We attribute the inadequate testing controls and Work Breakdown Structure to a lack of basic project management skills and qualifications. The project managers assigned to this project did not have the necessary skills to lead a project of this complexity.

## *Recommendations*

To ensure that basic project management practices are followed, the Chief Technology Officer should:

***Recommendation 1:*** Provide training to the FDCC project managers to ensure their project management skills and qualifications are sufficient.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS Chief Technology Officer will provide the FDCC project leaders with project management training to ensure their skills and qualifications are sufficient.

***Recommendation 2:*** Instruct the FDCC project leaders to develop and maintain an accurate master control list of all applications that require testing. The master control list should be frequently updated to account for software applications that are developed in-house or acquired from vendors. The master control list should also be updated with the test results for each application to verify that each application is tested and to maintain an accurate and timely information base for all test results.

> ***Management's Response:*** The IRS agreed with this recommendation and will ensure the master control list of applications is maintained and updated to account for software applications that are developed in-house or acquired from a vendor. The master control list will be updated with test results to indicate which applications have been tested and will be maintained as an accurate and timely information base.

## An Automated Monitoring Tool Was Not Implemented to Detect Changes to Workstation Security Settings

Long before the issuance of FDCC requirements by the OMB, the IRS had been required to monitor the security configuration settings on IRS workstations. The task of monitoring computer settings is paramount to ensure that once secure settings have been implemented those settings have not been improperly changed. In a previous review[13] of the IRS common operating environment, we reported that security settings were not consistently maintained once installed. In that report we found that, of our sample of 102 computers with the common operating environment image installed, only 42 were secure. The remaining 60 computers complied with less than 90 percent of the computer settings prescribed by the IRS or contained at least 1 high-risk vulnerability that could be exploited to either take control of the computer or render it unusable. We attributed the weak security settings to system administrators because they are the only persons authorized to change the security settings on employee workstations.

***The IRS spends an average of $2 million each year to perform monthly scans on a sample of computers to detect unauthorized changes to security settings.***

To detect and monitor changes to its common operating environment, the IRS uses the Windows Policy Checker[14] product. This tool is used to perform monthly scans on a sample of computers to detect unauthorized changes to security settings. However, the tool is labor intensive and the Modernization and Information Technology Services Division spends an average of $2 million each year to operate the tool. In May 2007, the IRS initiated the Security Compliance Posture Monitoring and Reporting Project to develop an automated enterprise approach to monitor security settings and manage information technology assets. Part of the project included acquiring an automated tool, validated by the National Institute of Standards and Technology, to monitor configuration settings. The tool would be used to automatically scan computers throughout the IRS network.

The OMB created a greater sense of urgency when it required[15] Federal Government agencies to monitor the FDCC settings by acquiring and using a tool compliant with the National Institute of Standards and Technology's Security Content Automation Protocol.[16] The Department of the Treasury reinforced the OMB requirement by setting an implementation deadline of

[13] *Secure Configurations Are Initially Established on Employee Computers, but Enhancements Could Ensure Security Is Strengthened After Implementation* (Report Reference 2006-20-031, dated February 2006).
[14] A tool used to determine whether systems are adhering to security policies.
[15] Memorandum for Chief Information Officers, *Establishment of Windows XP and VISTA Virtual Machine and Procedures for Adopting the Federal Desktop Core Configurations*, dated July 31, 2007.
[16] A method for using specific standards to enable automated vulnerability measurement and policy compliance evaluation. It is used to enumerate software flaws and security-related configuration issues.

January 31, 2008. However, the IRS has not complied with the OMB and Department of the Treasury requirements and has not purchased an approved scanning tool.

The delay in implementing the automated monitoring tool is due to a change in acquisition strategy. The IRS attempted to establish a sole-source contract to save time and costs in the acquisition process. However, in October 2008, the IRS Procurement Review Board rejected the sole-source procurement strategy and required the IRS to use an open-competition procurement.

The IRS' initial plan was to complete the Security Compliance Posture Monitoring and Reporting acquisition and deploy the monitoring tool in December 2009. However, the change in acquisition strategy will cause an additional delay. As of October 1, 2008, the IRS had not completed a request for proposal, which is a crucial first step in acquiring the product.

Until an automated enterprise monitoring tool is implemented, the IRS will 1) be vulnerable to unauthorized changes to its security settings, 2) be noncompliant with the OMB and Department of the Treasury requirements, and 3) incur maintenance costs for its outdated and labor-intensive Windows Policy Checker tool. In addition, it will be unable to monitor compliance with the FDCC settings throughout the organization. These risks increase the need to acquire a monitoring tool in a more timely manner than can be achieved through the Security Compliance Posture Monitoring and Reporting acquisition.

A viable alternative to the current acquisition strategy might be the General Services Administration's Government-wide blanket purchase agreement, referred to as the SmartBuy Program. The SmartBuy Program allows Federal Government agencies to select from an approved list of information technology vendors that provide security products with the ability to monitor and report on FDCC compliance. The security products have been validated as compliant with the National Institute of Standards and Technology's Security Content Automation Protocol guidelines.

## Recommendation

***Recommendation 3*:** The Chief Technology Officer should conduct an analysis of the costs and benefits of separating the purchase of the automated monitoring tool from the Security Compliance Posture Monitoring and Reporting acquisition. The cost-benefit analysis would allow the IRS to decide whether to purchase the tool from the General Services Administration's SmartBuy Program.

> ***Management's Response*:** The IRS agreed with this recommendation. The Chief Technology Officer will perform a cost-benefit analysis and request senior Modernization and Information Technology Services Division leadership to consider whether the purchase of a separate monitoring tool through the General Services Administration's SmartBuy Program would be in the IRS' best interest.

## Software Contracts Were Not Modified to Ensure Software Acquisitions Operate Properly With Federal Desktop Core Configuration Settings

The Federal Acquisition Regulation requires Federal Government agencies to include specific language in contracts for information technology purchases. When acquiring information technology, agencies must include the appropriate information technology security policies and requirements, including the common security configurations available from the National Institute of Standards and Technology.

The Department of the Treasury also requires the IRS to include specific FDCC language in software contracts. The new contract language recommended by the Department of the Treasury is intended to ensure that new acquisitions include common security configurations and that information technology providers certify that their products operate effectively using these configurations. The Department of the Treasury specified the following recommended language as a guide for agencies to use in their contracts:

> "*a) The provider of information technology shall certify applications are fully functional and operate correctly as intended on systems using the Federal Desktop Core Configuration (FDCC). This includes Internet Explorer 7 configured to operate on Windows XP and Vista.*
>
> *b) The standard installation, operation, maintenance, updates, and/or patching*[17] *of software shall not alter the configuration settings from the approved FDCC configuration…*"

The Department of the Treasury guidance was issued in June 2007. However, the IRS has not fully adopted the new FDCC contract language. We identified 27 (90 percent) of 30 contracts for new software products, including software upgrades and maintenance contracts, which did not include the required FDCC contract language. The three contracts that included the new FDCC language were uniquely processed because the contracts were sent by IRS business units directly to the Cybersecurity office for review rather than to the IRS Procurement Division.[18] The Cybersecurity office ensured the FDCC language was incorporated into the contracts prior to the contracts being forwarded to the Procurement Division. The 27 contracts that did not include the required FDCC language were not forwarded to the Cybersecurity office for review. These contracts totaled more than $15.8 million and included software products such as:

- VMware Workstation – A management tool for system administrators to enable control, configuration, monitoring, and troubleshooting a virtual server.

[17] A patch is a fix of a design flaw in a computer program. Patches must be installed or applied to the appropriate computer for the flaw to be corrected.
[18] The Procurement Division is part of the IRS Agency-Wide Shared Services Division.

- Brava! Enterprise – Software that provides secure content visualization and annotation for the IRS' internal and external web sites.
- SecureDoc – Software that is used for full disk encryption to protect sensitive information stored on laptop and desktop computers.

The IRS did not place sufficient emphasis on implementing the requirement to adopt the FDCC contract language into its contracts. As a result, the IRS has not contractually obligated vendors to provide applications and software products that operate as intended with the FDCC. As a result, the IRS may be procuring software products that are not secure and would need to expend additional resources to correct deficiencies. If acquired software products are tested and found to be incompatible with the FDCC, the IRS would not have adequate recourse and the vendor would have the right to demand payment.

## Recommendation

***Recommendation 4:*** The Chief Technology Officer should direct the Cybersecurity office to coordinate with the Procurement Division and prioritize the work that is necessary to include the required FDCC contract language in information technology acquisitions.

> ***Management's Response:*** The IRS agreed with this recommendation and will ensure affected stakeholders coordinate and prioritize the work that is necessary to issue an agency-wide policy and interim acquisition procedures that incorporate the FDCC contract language into information technology acquisitions.

## Appendix I

# Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether the IRS has made adequate progress in implementing required Federal secure configurations on employee computers. These Federal secure configurations are referred to as the FDCC. To accomplish our objective, we:

I. Identified the FDCC security settings that the National Institute of Standards and Technology[1] published for Federal Government computers running Windows XP and determined the cause for any delays in implementing the settings.

A. Reviewed the National Institute of Standards and Technology checklist to identify the required FDCC settings. We determined when the checklist was finalized and made available to Federal Government agencies.

B. Reviewed the Internal Revenue Manual and compared it to the FDCC settings to determine how many FDCC settings were established in IRS procedures prior to the FDCC being required.

C. Evaluated the stability of the National Institute of Standards and Technology checklist and identified changes that were made after initial publication of the checklist.

D. Interviewed End User Equipment and Services organization project personnel to determine whether the IRS completed an initial FDCC compliance assessment and established a project team in a timely manner.

E. Interviewed project leaders to determine whether the FDCC project team had adequate executive leadership and oversight during the early phases of the project.

II. Evaluated the End User Equipment and Services organization project team's testing methodology to determine whether the current testing is adequate to adopt the highest possible number of FDCC settings in a timely manner.

A. Interviewed the End User Equipment and Services organization lab team and obtained a walk-through of their testing methodology. We determined whether the

[1] The National Institute of Standards and Technology, 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.

current testing methodology will identify potential problems if the FDCC settings are installed in the common operating environment.[2] We determined:

1. The number of FDCC settings that have been tested and approved.
2. The scope of the testing.
3. How the applications are tested, i.e., tested in isolation or while operating simultaneously with other applications running in the user environment.
4. Whether the test environments used for testing are representative of actual IRS operating environments.
5. How the settings are passed or deemed acceptable for the IRS common operating environment.
6. The number of settings implemented, via Active Directory, on IRS computers.

B. Interviewed project personnel to determine why the first testing methodology was unsuccessful and how much of a delay the failed test methodology caused.

C. Evaluated the Work Breakdown Structure to determine whether the timetable for testing all FDCC settings is feasible.

D. Analyzed test reports to verify that the test team documented and analyzed results.

E. Determined how the Security Content Automation Protocol[3] testing tool operates and its effect on the FDCC implementation efforts.

F. Evaluated the procedures the lab follows to control and address the problems/issues that are identified in the test environment.

III. Evaluated the implementation of FDCC settings in the IRS computing environment to determine whether the IRS installed the settings that were tested and approved by the End User Equipment and Services organization project team.

A. Interviewed project team personnel and reviewed documentation to determine whether the IRS has made progress in implementing the FDCC settings.

B. Evaluated justifications for FDCC deviations to determine whether they were warranted.

[2] To ensure consistency across the IRS network and improve security, the IRS created the common operating environment, which is a standardized set of commercial off-the-shelf and internally developed applications to support the needs of all IRS employees using Microsoft Windows. The common operating environment also allows the IRS to control security configuration settings and software on its workstations by changing one master template and then installing it on all computer workstations throughout the agency.

[3] A method for using specific standards to enable automated vulnerability measurement and policy compliance evaluation. It is used to enumerate software flaws and security-related configuration issues.

IV. Evaluated the controls and tools used by the End User Equipment and Services organization to monitor compliance with the FDCC settings that have been put in place.

A. Determined whether the IRS had taken corrective actions to address the issues in our audit report *Secure Configurations Are Initially Established on Employee Computers, but Enhancements Could Ensure Security Is Strengthened After Implementation* (Reference Number 2006-20-031, dated February 2006).

B. Interviewed the project team to determine whether the IRS had automated the enforcement of the FDCC settings.

C. Interviewed project personnel to determine how the End User Equipment and Services organization restricts administration of the configuration settings.

D. Determined whether the IRS established a process to ensure acquisitions made after June 2007 include the FDCC settings and that information technology vendors certify that their products operate effectively using the configurations.

## Appendix II

# Major Contributors to This Report

Margaret Begg, Acting Assistant Inspector General for Audit (Security and Information Technology Services)
Stephen Mullins, Director
Kent Sagara, Acting Director
W. Allen Gray, Audit Manager
Cari Fogle, Senior Auditor
George Franklin, Senior Auditor
Bret Hunter, Senior Auditor
Esther Wilson, Senior Auditor

## Appendix III

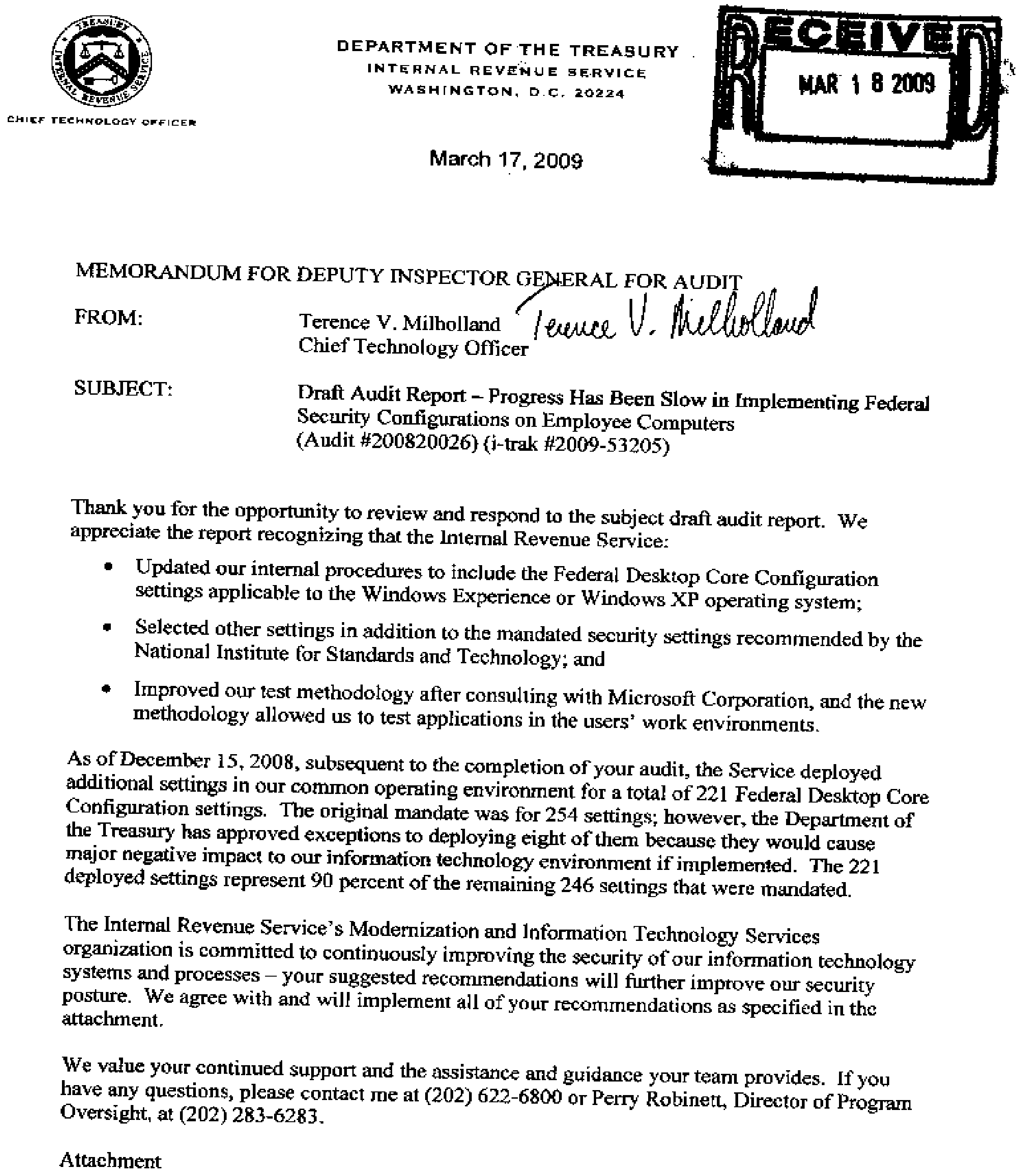
# *Report Distribution List*

Commissioner  C
Office of the Commissioner – Attn:  Chief of Staff  C
Deputy Commissioner for Operations Support  OS
Chief Information Officer  OS:CIO
Associate Chief Information Officer, Cybersecurity  OS:CIO:C
Associate Chief Information Officer, End User Equipment and Services  OS:CIO:EUES
Director, Stakeholder Management Division  OS:CIO:SM
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 Liaisons:

- Chief Information Officer  OS:CIO
- Associate Chief Information Officer, Cybersecurity  OS:CIO:C
- Associate Chief Information Officer, End User Equipment and Services  OS:CIO:EUES
- Director, Program Oversight  OS:CIO:SM:PO

## Appendix IV

# Management's Response to the Draft Report



CHIEF TECHNOLOGY OFFICER

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

March 17, 2009

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Terence V. Milholland Terence V. Milholland
Chief Technology Officer

SUBJECT: Draft Audit Report – Progress Has Been Slow in Implementing Federal Security Configurations on Employee Computers
(Audit #200820026) (i-trak #2009-53205)

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

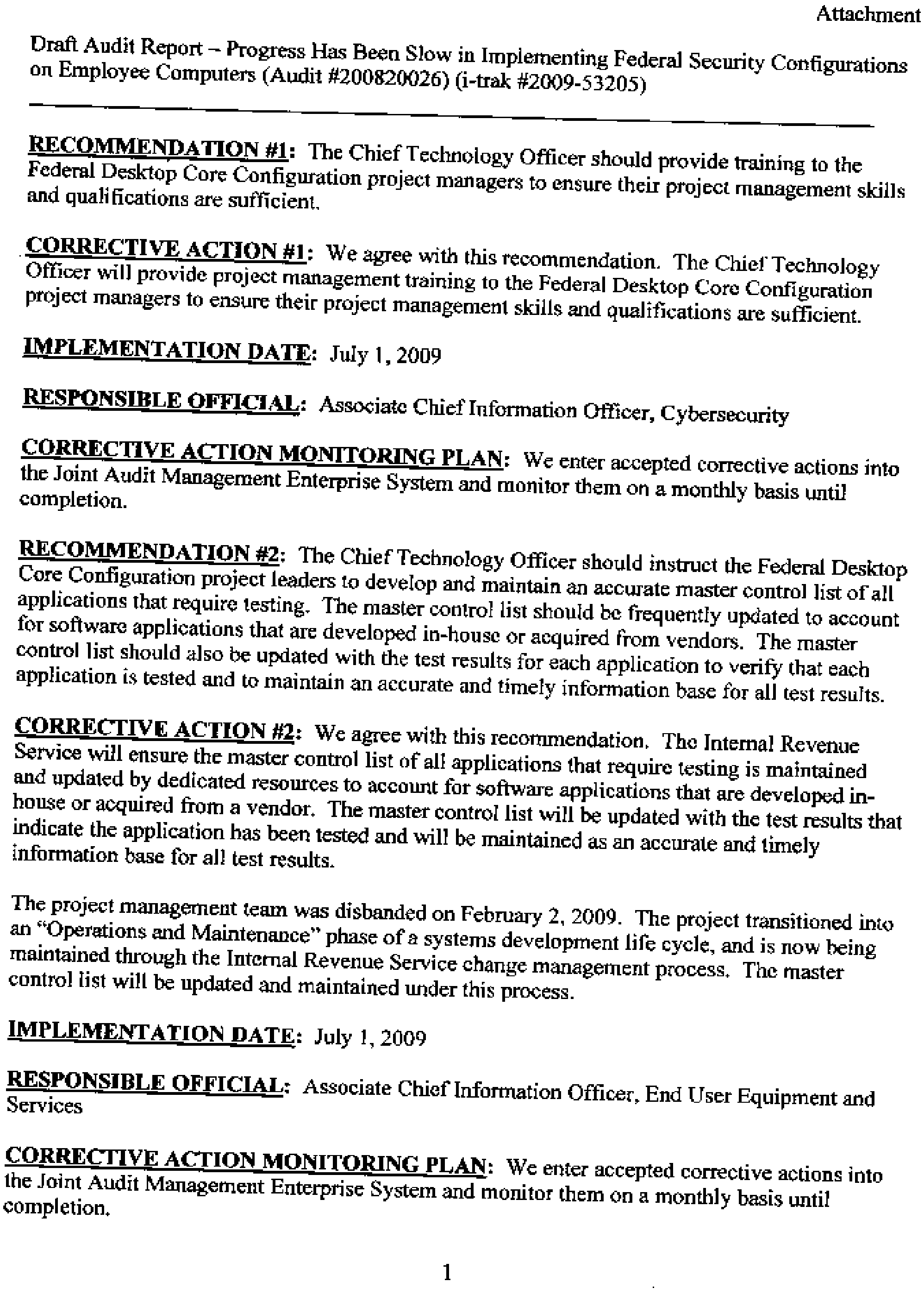
- Updated our internal procedures to include the Federal Desktop Core Configuration settings applicable to the Windows Experience or Windows XP operating system;
- Selected other settings in addition to the mandated security settings recommended by the National Institute for Standards and Technology; and
- Improved our test methodology after consulting with Microsoft Corporation, and the new methodology allowed us to test applications in the users' work environments.

As of December 15, 2008, subsequent to the completion of your audit, the Service deployed additional settings in our common operating environment for a total of 221 Federal Desktop Core Configuration settings. The original mandate was for 254 settings; however, the Department of the Treasury has approved exceptions to deploying eight of them because they would cause major negative impact to our information technology environment if implemented. The 221 deployed settings represent 90 percent of the remaining 246 settings that were mandated.

The Internal Revenue Service's Modernization and Information Technology Services organization is committed to continuously improving the security of our information technology systems and processes – your suggested recommendations will further improve our security posture. We agree with and will implement all of your recommendations as specified in the attachment.

We value your continued support and the assistance and guidance your team provides. If you have any questions, please contact me at (202) 622-6800 or Perry Robinett, Director of Program Oversight, at (202) 283-6283.

Attachment



Attachment

Draft Audit Report – Progress Has Been Slow in Implementing Federal Security Configurations on Employee Computers (Audit #200820026) (i-trak #2009-53205)

**RECOMMENDATION #1**: The Chief Technology Officer should provide training to the Federal Desktop Core Configuration project managers to ensure their project management skills and qualifications are sufficient.

**CORRECTIVE ACTION #1**: We agree with this recommendation. The Chief Technology Officer will provide project management training to the Federal Desktop Core Configuration project managers to ensure their project management skills and qualifications are sufficient.

**IMPLEMENTATION DATE**: July 1, 2009

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

**CORRECTIVE ACTION MONITORING PLAN**: We enter accepted corrective actions into the Joint Audit Management Enterprise System and monitor them on a monthly basis until completion.

**RECOMMENDATION #2**: The Chief Technology Officer should instruct the Federal Desktop Core Configuration project leaders to develop and maintain an accurate master control list of all applications that require testing. The master control list should be frequently updated to account for software applications that are developed in-house or acquired from vendors. The master control list should also be updated with the test results for each application to verify that each application is tested and to maintain an accurate and timely information base for all test results.

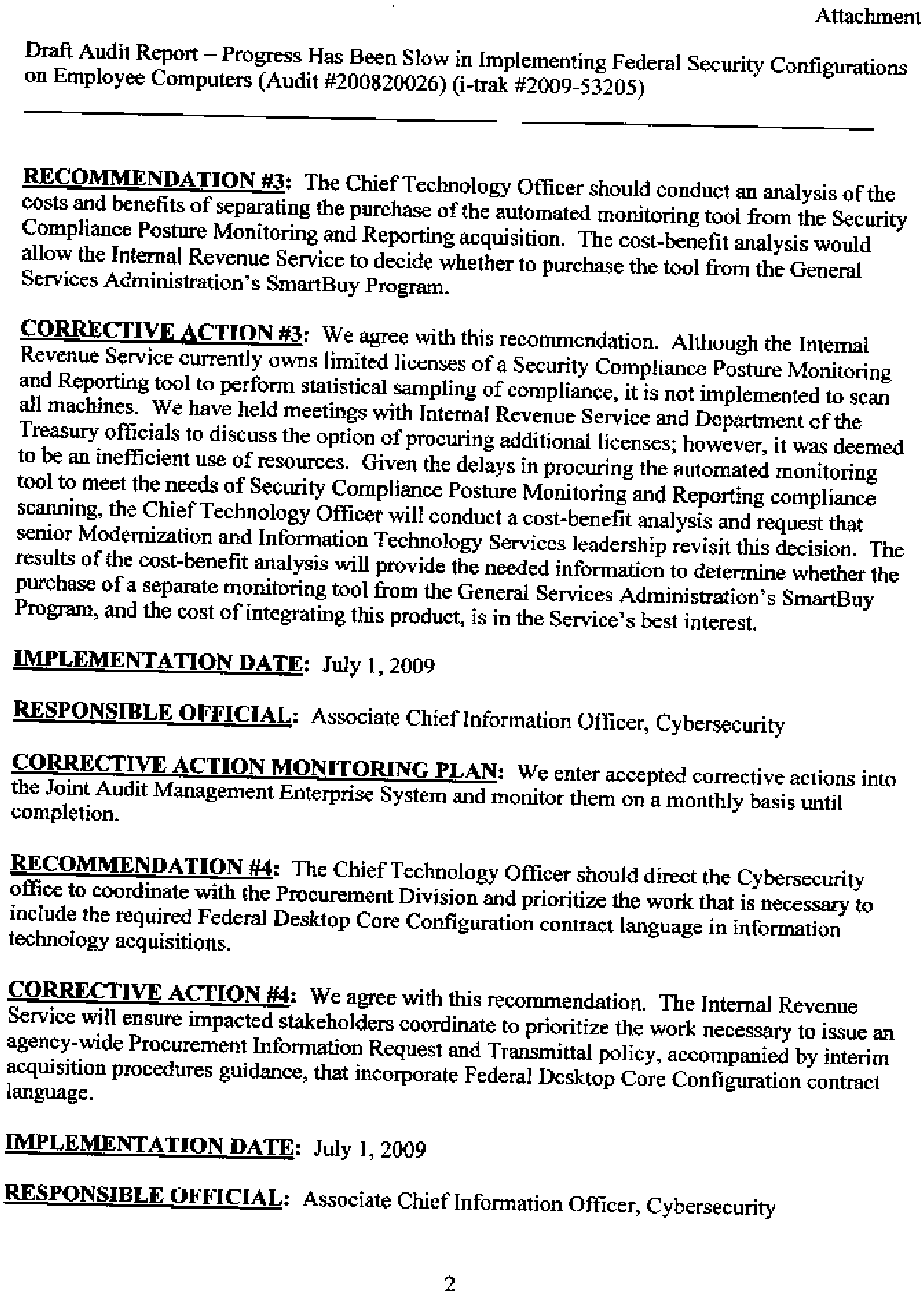
**CORRECTIVE ACTION #2**: We agree with this recommendation. The Internal Revenue Service will ensure the master control list of all applications that require testing is maintained and updated by dedicated resources to account for software applications that are developed in-house or acquired from a vendor. The master control list will be updated with the test results that indicate the application has been tested and will be maintained as an accurate and timely information base for all test results.

The project management team was disbanded on February 2, 2009. The project transitioned into an "Operations and Maintenance" phase of a systems development life cycle, and is now being maintained through the Internal Revenue Service change management process. The master control list will be updated and maintained under this process.

**IMPLEMENTATION DATE**: July 1, 2009

**RESPONSIBLE OFFICIAL**: Associate Chief Information Officer, End User Equipment and Services

**CORRECTIVE ACTION MONITORING PLAN**: We enter accepted corrective actions into the Joint Audit Management Enterprise System and monitor them on a monthly basis until completion.



Attachment

Draft Audit Report – Progress Has Been Slow in Implementing Federal Security Configurations on Employee Computers (Audit #200820026) (i-trak #2009-53205)

**RECOMMENDATION #3:** The Chief Technology Officer should conduct an analysis of the costs and benefits of separating the purchase of the automated monitoring tool from the Security Compliance Posture Monitoring and Reporting acquisition. The cost-benefit analysis would allow the Internal Revenue Service to decide whether to purchase the tool from the General Services Administration's SmartBuy Program.

**CORRECTIVE ACTION #3:** We agree with this recommendation. Although the Internal Revenue Service currently owns limited licenses of a Security Compliance Posture Monitoring and Reporting tool to perform statistical sampling of compliance, it is not implemented to scan all machines. We have held meetings with Internal Revenue Service and Department of the Treasury officials to discuss the option of procuring additional licenses; however, it was deemed to be an inefficient use of resources. Given the delays in procuring the automated monitoring tool to meet the needs of Security Compliance Posture Monitoring and Reporting compliance scanning, the Chief Technology Officer will conduct a cost-benefit analysis and request that senior Modernization and Information Technology Services leadership revisit this decision. The results of the cost-benefit analysis will provide the needed information to determine whether the purchase of a separate monitoring tool from the General Services Administration's SmartBuy Program, and the cost of integrating this product, is in the Service's best interest.

**IMPLEMENTATION DATE:** July 1, 2009

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

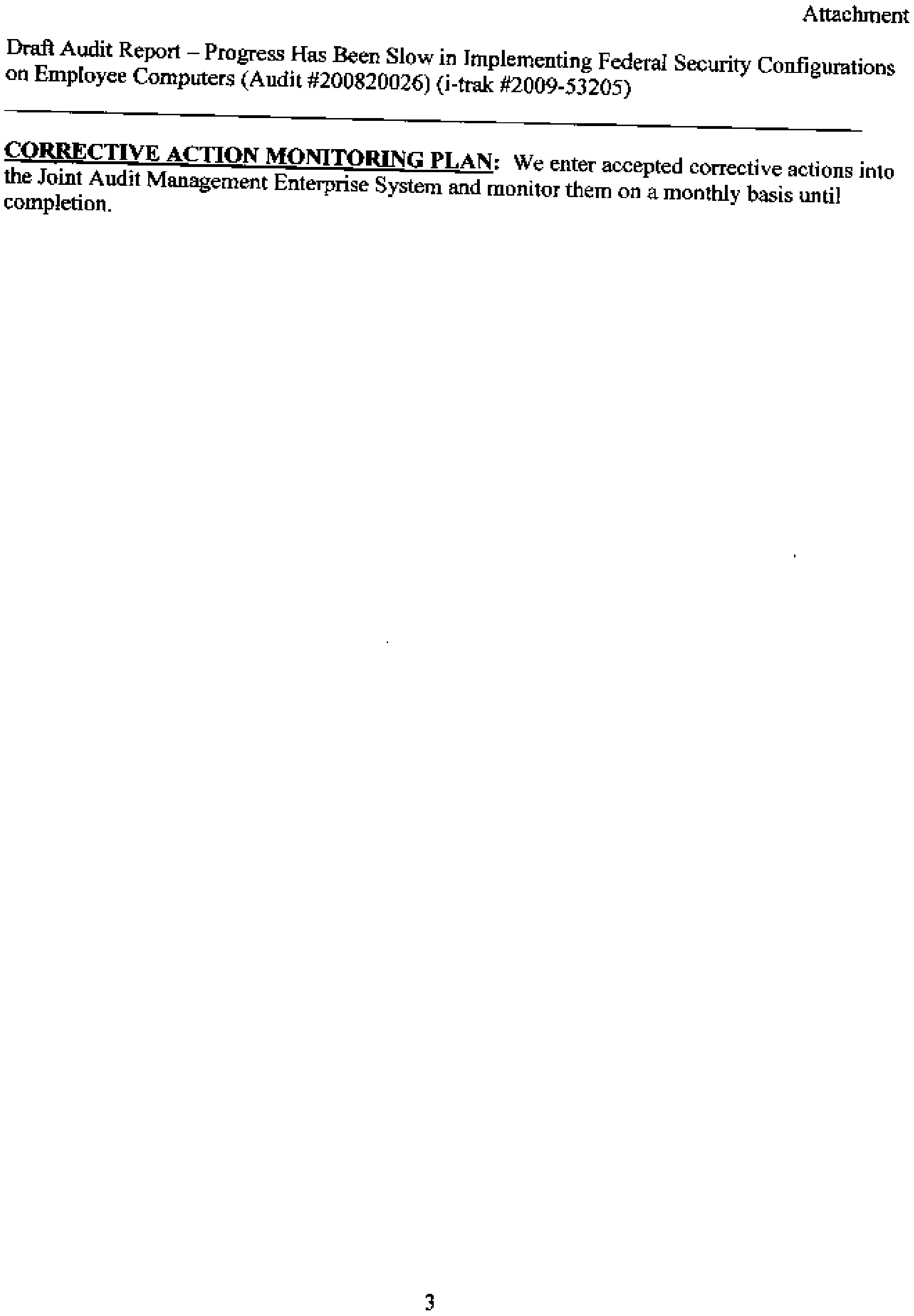
**CORRECTIVE ACTION MONITORING PLAN:** We enter accepted corrective actions into the Joint Audit Management Enterprise System and monitor them on a monthly basis until completion.

**RECOMMENDATION #4:** The Chief Technology Officer should direct the Cybersecurity office to coordinate with the Procurement Division and prioritize the work that is necessary to include the required Federal Desktop Core Configuration contract language in information technology acquisitions.

**CORRECTIVE ACTION #4:** We agree with this recommendation. The Internal Revenue Service will ensure impacted stakeholders coordinate to prioritize the work necessary to issue an agency-wide Procurement Information Request and Transmittal policy, accompanied by interim acquisition procedures guidance, that incorporate Federal Desktop Core Configuration contract language.

**IMPLEMENTATION DATE:** July 1, 2009

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



Attachment

Draft Audit Report – Progress Has Been Slow in Implementing Federal Security Configurations on Employee Computers (Audit #200820026) (i-trak #2009-53205)

**CORRECTIVE ACTION MONITORING PLAN:** We enter accepted corrective actions into the Joint Audit Management Enterprise System and monitor them on a monthly basis until completion.