Using SmartID Cards to Access Computer Systems Is Taking Longer Than Expected

September 28, 2012

Reference Number: 2012-20-115

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

USING SMARTID CARDS TO ACCESS COMPUTER SYSTEMS IS TAKING LONGER THAN EXPECTED

Highlights

Final Report issued on September 28, 2012

Highlights of Reference Number: 2012-20-115 to the Internal Revenue Service Chief Technology Officer.

IMPACT ON TAXPAYERS

The President's Cyberspace Policy emphasized that agencies need to use SmartID cards to access computer systems. The IRS's efforts to upgrade its systems to use the SmartID cards are taking longer than expected. Upgrading the security of computer systems is important to prevent disruptions in critical IRS processes and to protect taxpayers' personal information from unauthorized access.

WHY TIGTA DID THE AUDIT

This audit was initiated to evaluate the implementation and security of the IRS's two-factor authentication system for accessing computer systems. Two-factor authentication is a secure approach to verifying employees' identities on a system and requires the presentation of two identifying factors: something the user knows (a personal identification number) and something the user has (a SmartID card). Two-factor authentication provides significant improvement in computer security in terms of allowing access to systems.

WHAT TIGTA FOUND

The IRS developed a two-factor authentication system with the required components. However, significant delays prevented the IRS from deploying the new two-factor authentication system as originally planned. The IRS originally planned to complete the deployment by September 2011. The deployment is now planned to be completed by July 2013.

In addition, the IRS did not appoint a project manager with the requisite training and experience to lead the Internal Identity and Access Management project, which included the two-factor authentication component. This decision led to numerous issues. The project team did not make adequate progress in some crucial areas such as developing two-factor authentication for computer administrators, conducting required testing, and completing key documents and processes.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Technology Officer direct IRS Labor Relations to notify the National Treasury Employees Union and begin negotiating mandatory use of the SmartID cards. TIGTA also recommended that the Assistant Chief Information Officer, Cybersecurity, appoint a certified project manager with the requisite training and experience to lead the Internal Identity and Access Management project and direct the project manager to ensure the required security control assessment is completed, select a method to implement two-factor authentication for administrators, coordinate the activities to ensure all required testing is completed, and complete the required documents and processes that are needed to fully test and evaluate the system.

The IRS agreed with seven of the recommendations and plans to bargain with the National Treasury Employees Union as appropriate on mandatory use of the SmartID Cards, appoint a certified project manager and provide adequate resources to the project, and assign project resources to determine if a viable solution for administrators' use of SmartID cards exists. The IRS disagreed with two recommendations regarding the required testing of the new system and stated that testing was completed in accordance with its procedures and additional testing is not necessary.

TIGTA remains concerned about the IRS's disagreement on the issue of testing. The IRS did not conduct the required testing for the most significant part of the two-factor authentication system, which is the part employees will use to authenticate to the IRS network. TIGTA found no evidence that the security, integration, capacity, and performance testing were conducted for this crucial part of the system.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

September 28, 2012

MEMORANDUM FOR CHIEF TECHNOLOGY OFFICER

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

SUBJECT: Final Audit Report – Using SmartID Cards to Access Computer Systems Is Taking Longer Than Expected (Audit # 201120011)

This report presents the results of our review of the Internal Revenue Service's efforts to implement the use of SmartID card access for computer systems. This audit is included in our Fiscal Year 2012 Annual Audit Plan and addresses the major management challenge of Security for Taxpayer Data and Employees.

Management's complete response to the draft report is included in Appendix VIII. The response details the Internal Revenue Service's disagreement with two recommendations and indicates the required testing was not conducted prior to deploying the two-factor authentication system using SmartID cards. In addition, responses to other recommendations indicate this project is not being given sufficient priority. Because we believe the Internal Revenue Service's disagreements to our findings and recommendations are significant, we plan to elevate our concerns to the Department of the Treasury. We request that the IRS Commissioner submit a written reply to the Assistant Secretary for Management and Chief Financial Officer of the Department of the Treasury within 30 calendar days of the final report issuance date.

Copies of this report are also being sent to the Internal Revenue Service Managers affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions or Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services), at (202) 622-5894.

Table of Contents

Background ..... Page 1

Results of Review ..... Page 4

The Internal Revenue Service Developed a Two-Factor Authentication System With the Required Components ..... Page 4

The Internal Identity and Access Management Project Encountered Significant Delays ..... Page 5

A Project Manager Was Not Appointed to Manage the Internal Identity and Access Management Project ..... Page 7

Use of SmartID Cards Will Be Further Delayed ..... Page 7

Recommendation 1: ..... Page 10

Recommendations 2 through 4: ..... Page 11

Recommendation 5: ..... Page 12

Required Testing Was Not Conducted ..... Page 12

Key Enterprise Life Cycle Artifacts and Processes Were Not Completed ..... Page 14

Recommendations 6 through 8: ..... Page 18

Recommendation 9: ..... Page 19

Appendices

Appendix I – Detailed Objective, Scope, and Methodology ..... Page 20

Appendix II – Major Contributors to This Report ..... Page 23

Appendix III – Report Distribution List ..... Page 24

Appendix IV – Authentication to Network Diagram ..... Page 25

Appendix V – Diagram of Oracle Enterprise Single Sign-On Manager Software ..... Page 26

Appendix VI – Delays in Implementing Reduced SmartID Sign-On (RSSO) .....Page 27

Appendix VII – Glossary of Terms .....Page 28

Appendix VIII – Management's Response to the Draft Report .....Page 34

Abbreviations

ELC	Enterprise Life Cycle
ESSO	Enterprise Single Sign-On Manager
FY	Fiscal Year
HSPD	Homeland Security Presidential Directive
IIAM	Internal Identity and Access Management
IRS	Internal Revenue Service
MRR	Milestone Readiness Review
OMB	Office of Management and Budget
PIV	Personal Identity Verification
RSSO	Reduced SmartID Sign-On

Background

On August 27, 2004, President Bush signed Homeland Security Presidential Directive-12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*. This directive established a new standard for issuing and maintaining identification badges for Federal employees and contractors entering Government facilities and accessing computer systems.[1] The intent was to improve security, increase Government efficiency, reduce identity fraud, and protect personal privacy. Agencies are required to use Personal Identity Verification (PIV) badges (also referred to as SmartID cards) to access computer systems (logical access).

Over the past five years, the HSPD-12 mandate has been emphasized continuously.

- The Department of the Treasury (hereafter called the Treasury Department) issued Treasury Directive 85-01, *Treasury Information Technology Security Program*,[2] establishing Security Enhanced Controls 14 and 15. Security Enhanced Control 14 mandates two-factor authentication for access to all administrator accounts and Security Enhanced Control 15 requires bureaus to design authentication methods with HSPD-12 credentials for access to all systems.
- The *President's Cyberspace Policy Review*, issued in May 2009, and the President's budget for Fiscal Year (FY) 2011 highlighted the importance of identity management in protecting the Nation's infrastructure.
- The Office of Management and Budget (OMB), in February 2011, emphasized the continued implementation of HSPD-12 by requiring that SmartID cards be used as the common means of authentication for access to the agency's facilities, networks, and information systems.[3] The OMB also required agencies to follow specific technical standards and business processes for the issuance and routine use of the SmartID cards.
- In the same OMB February 2011 memorandum, the Department of Homeland Security required agencies to develop an implementation plan to expedite the full use of the SmartID cards as the common means of authentication for access to networks and information systems. Effective at the beginning of FY 2012, existing logical access control systems must be upgraded to use SmartID cards prior to the agency using development and technology funds to complete other activities.

[1] See Appendix VII for a glossary of terms used throughout this report.
[2] Department of the Treasury, Treasury Directive Publication 85-01 (Rev. 2.2), *Treasury Information Technology Security Program* (Nov. 2006, includes updates as of March 1, 2012).
[3] OMB, Memorandum 11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors* (Feb. 2011).

The Internal Revenue Service (IRS) is addressing the logical access portion of the HSPD-12 mandate and Treasury Department's two-factor authentication directive through its Internal Identity and Access Management (IIAM) program. Phase 2 of this program (hereafter called the IIAM project) includes designing, developing, and deploying the capability of employees to use SmartID cards to authenticate to:

- The Windows® network.
- Administrator accounts, which provide elevated access privileges.
- The IRS's virtual private network, known as the Enterprise Remote Access Project, which is used by employees working in remote locations. The grid cards currently used to authenticate to this virtual private network must be replaced with SmartID cards.
- Mainframe systems.

The IRS plans for 50,000 employees to use their SmartID card for logical access by the end of December 2012.

System security will be significantly improved at the IRS once employees are using SmartID cards for logical access. Users will insert their SmartID card into a card reader connected to the computer or into a built-in card reader slot that is present on some computers and, when prompted, type in their personal identification number. The software on the computer verifies the SmartID card and personal identification number by communicating with a database located at the Treasury Department's Bureau of the Public Debt. See Appendix IV for a diagram of the authentication system the IRS developed to use SmartID cards for logging on to the network.

The scope of the IIAM project also includes deployment of the Oracle Enterprise Single Sign-On Manager (Oracle ESSO) software to computer workstations and laptop computers. This commercial off-the-shelf software is intended to provide a short-term solution to further reduce the use of passwords when accessing IRS applications. However, IIAM project officials informed us that this software is not the long-term solution for authenticating employees to IRS applications. See Appendix V for a diagram of how the Oracle ESSO operates. IIAM project officials report to the IRS's Security Services and Privacy Executive Steering Committee, which provides oversight and approves the project's Enterprise Life Cycle (ELC) Milestone Exit Reviews.

This review was focused on the IRS's efforts to implement two-factor authentication for its network using SmartID cards. We performed the review in the offices of the Information Technology organization in New Carrollton, Maryland, and Martinsburg, West Virginia, from January through June 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.

Results of Review

The Internal Revenue Service Developed a Two-Factor Authentication System With the Required Components

Implementation policies were updated – The IRS updated its implementation policies consistent with the Treasury Department and Department of Homeland Security directives. These policies are intended to help the IRS expedite the use of SmartID cards for logical access and to comply with Federal mandates. The IRS made the following updates to its policies:

- Effective the beginning of Fiscal Year 2012, existing physical and logical access control systems must be upgraded to use PIV credentials, in accordance with National Institute of Standards and Technology guidelines, prior to the agency using technology refresh funds to complete other activities.
- Procurements for services and products involving facility or system access control must be in accordance with HSPD-12 policy and the Federal Acquisition Regulations. In order to ensure Government-wide interoperability, OMB Memorandum 06-18, *Acquisition of Products and Services for Implementation of HSPD-12*, dated June 6, 2006, requires agencies to acquire products and services that are approved as compliant with Federal policy, standards, and supporting technical specifications.
- Effective immediately, all new systems under development must be enabled to use PIV credentials, in accordance with National Institute of Standards and Technology guidelines, prior to being made operational.
- Agency processes must accept and electronically verify PIV credentials issued by other Federal agencies.
- The Government-wide architecture and completion of agency transition plans must align as described in the Federal Chief Information Officer Council's *Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance*, dated November 10, 2009.

The two-factor authentication system included the required components – The IRS's two-factor authentication system includes the three main components required by Federal Information Processing Standard Publication 201.[4] These components include:

[4] National Institute of Standards and Technology, FIPS PUB 201-1, *Federal Information Processing Standards Publication: Personal Identity Verification of Federal Employees and Contractors* (Mar. 2006).

- PIV Front-End Subsystem – PIV cards, card readers, and personal identification number input devices. The PIV cardholder interacts with these components to gain logical access to the desired Federal resource.
- PIV Card Issuance and Management Subsystem – the components responsible for identity proofing and registration, card and key issuance and management, and various repositories and services required as part of the verification infrastructure.
- Access Control Subsystem – the logical access control systems, the protected resources, and the authorization data.

The IRS acquired products that are compliant with technical specifications

- The ActivClient middleware used to read the SmartID cards is certified by the National Institute of Standards and Technology.
- The Oracle ESSO software is an approved product in the IRS Enterprise Architecture.
- The external card readers purchased to read the SmartID cards are personal computer/SmartID card certified.

The combination of the card readers and the ActivClient middleware enables users to authenticate to the network using their SmartID cards.

As previously stated, the Oracle ESSO software is an interim solution until a more significant change to the IRS's infrastructure can be implemented. The software is not certified by the National Institute of Standards and Technology and does not reduce the number of identity stores at the IRS. The IRS's final solution will reduce the number of identity stores and allow system administrators to efficiently add and remove users' access to applications. Reducing the number of identity stores the IRS has will also reduce the risk of unauthorized access to systems.

The Internal Identity and Access Management Project Encountered Significant Delays

The IRS is 22 months behind its original planned completion date for implementing the new two-factor authentication system and enabling all employees to use SmartID cards for logical access. The original completion date was September 30, 2011, but the IRS now expects to fully complete the implementation by July 26, 2013. The following delays prevented the IRS from implementing the IIAM project on time. See Appendix VI for a timeline of these delays.

The encryption requirements changed – The IRS successfully upgraded the level of encryption for the certificates on the SmartID cards from secure hash algorythym-1 to secure hash algorythum-256 to meet the requirements recommended by the National Institute of Standards

and Technology.[5] The IRS initially believed it could not support the stronger encryption standards and would be forced to upgrade its Windows XP operating system on all computer workstations. However, the IRS coordinated with the Microsoft Corporation to obtain a service patch that made the operating system compatible with the new encryption standard.

The Oracle Corporation acquired Passlogix – When the IRS originally procured the Oracle ESSO software in August 2010, this software was named v-GO SSO and was owned by a company named Passlogix. In October 2010, the Oracle Corporation purchased Passlogix and rebranded the software to reflect the new owner. This change caused problems in the software, and it ceased to function as intended. The IRS's reliance on the Oracle Corporation to address these issues took a considerable amount of time and caused additional delays.

Negotiations with the National Treasury Employees Union – The IRS is required to negotiate with the National Treasury Employees Union when the IRS initiates changes to employees' working conditions. Negotiations with the Union to implement the IIAM project took longer than expected due to three issues.

1. **Discipline** – Managing employees who repeatedly lose their SmartID card, who are repeatedly locked out of their accounts, and who gain inappropriate access to the network.
2. **Communication Packet** – Issuing a "communication packet" to employees with instructions on how to use the Reduced SmartID Sign-On capability (RSSO).[6] The packet must be issued to all affected employees no less than five workdays before implementation.
3. **Unauthorized Access** – Adding the following statement to the Memorandum of Understanding that was signed by the IRS and the Union: "Bargaining unit employees will not be held responsible and/or disciplined if an employee's Reduced SmartID Sign-On system accesses an unauthorized system and/or network through no fault of the bargaining unit employee."

Filing Season Moratorium – Every year a filing season moratorium is put into place at the IRS to stabilize its production environments during peak processing times. During the moratorium, no changes to the production environment are allowed to be implemented without executive approval, and the IIAM project did not have this approval. In FY 2011, the moratorium was in effect from November 30, 2010, through May 23, 2011, and in FY 2012, from November 1, 2011, through May 21, 2012.

The Customer Account Data Engine, version 2, was a higher priority – On October 14, 2011, the IRS Information Technology organization's Enterprise Operations function requested that the

[5] National Institute of Standards and Technology, NIST Special Publication 800-78-3, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification* (Dec. 2010).
[6] The Reduced SmartID Sign-On is a significant part of the IIAM project and provides two separate yet related functions: 1) the capability to logon to the IRS network and 2) the capability to use the Oracle ESSO software.

IIAM project delay its deployment of the RSSO until May 2012. This request was due to the Enterprise Operations function's responsibility for ensuring the IRS Customer Account Data Engine 2 would operate as intended during the filing season. The Customer Account Data Engine 2 was a top priority, and the Enterprise Operations function could not afford for their computers to be inoperable due to any RSSO deployment issues. If the Customer Account Data Engine 2 went offline, returns could not be processed timely, and this was a risk that the Enterprise Operations function was not willing to take.

The cumulative effect of these delays resulted in the IRS acquiring software licenses that were not used. The IRS bought 95,000 ActivClient licenses, totaling $1,077,300, for use during the period August 31, 2010, through August 30, 2011. In addition, 95,000 licenses for the Oracle ESSO software were purchased for use during this same period for $1,452,550. The licenses were never used because the IRS did not begin deploying the software until May 2012.

The IRS bought the software licenses in August 2010 in the event the RSSO deployment could begin as originally planned in December 2010. Also, IIAM project officials wanted to use FY 2010 funds that were available at that time but might not be available in subsequent years.

A Project Manager Was Not Appointed to Manage the Internal Identity and Access Management Project

Many of the issues presented in the remaining sections of this report are due to the lack of a project manager with the requisite training and experience to manage the IIAM project. The IIAM project started in Calendar Year 2009 and was led by the Information Technology organization's Enterprise Services function. The Enterprise Services function did not have staffing resources to assign a project manager. After the project team completed its milestone exits in December 2010, the team members were reassigned to other projects, and leadership was assigned to the Information Technology organization's Cybersecurity office. At the end of our fieldwork in July 2012, a project manager had not been appointed to lead the numerous complex IIAM activities. A project manager was needed to: 1) oversee the progress in developing two-factor authentication for administrators, applications, and the virtual private network; 2) ensure the required testing was performed; and 3) ensure ELC artifacts and review processes required in the project's tailoring plan were properly completed.

Use of SmartID Cards Will Be Further Delayed

The use of SmartID cards for two-factor authentication will continue to experience delays due to the following reasons.

The IRS cannot require employees to use their SmartID cards for logical access

The IRS cannot require its employees to use their SmartID cards for logical access to the network because it did not negotiate mandatory use of the cards with the National Treasury

Employees Union. The Memorandum of Understanding signed by the IRS and the Union in October 2011 invites employees to use their SmartID cards on a voluntary basis. In addition, the IRS does not have a time period in place when it expects to mandate the use of the cards, nor has it begun negotiations with the Union to require usage.

The IRS's Information Technology organization directed the Labor Relations office not to negotiate mandatory use of the SmartID cards with the National Treasury Employees Union due to several reasons, such as the logistical problems some employees will face if they need to replace their damaged or lost SmartID card. Some employees work in close proximity to a SmartID card credentialing station, which facilitates a relatively easy card replacement process, while other employees work in remote offices. The Union did not want some employees to be required to use their SmartID cards while others are not required.

In a January 2011 memorandum to the Treasury Department, the OMB cited the department's lack of progress in using the SmartID cards to access computer systems. The OMB approved[7] funding for the Treasury Department's information technology development, modernization, and enhancement initiatives based on the completion of three goals related to SmartID card usage:

- 25 percent of SmartID cardholders must be using the cards for logical access to the network by the end of FY 2011.
- 50 percent of SmartID cardholders must be using the cards by the end of FY 2012.
- 100 percent of SmartID cardholders must be using the cards by the end of FY 2013.

The OMB approved development, modernization, and enhancement funding for activities only through FY 2012 and noted that, based on successful completion of the above goals, it would evaluate the appropriateness of funding for FY 2013 and beyond. The Treasury Department established the OMB's FY 2012 usage goal for the IRS.

Considering that the previous negotiations with the Union lasted approximately two years, the next round of negotiations to mandate use of the SmartID cards could take just as long or longer, which would further delay employees using their cards. Many employees could choose to continue using their passwords. The delays would postpone the security enhancements of two-factor authentication and could affect information technology funding due to not meeting the OMB SmartID card usage goals.

[7] Department of the Treasury, *Treasury Improvement Plan for Treasury Enterprise Identity, Credential and Management Investment* (Jan. 2011).

Inadequate progress implementing two-factor authentication for administrators

The Federal Identity and Credential Access Management Roadmap[8] requires agencies to ensure computer users authenticate to computer resources using one SmartID card. It also advises that if using the SmartID cards for administrator accounts is not technically feasible, agencies could use another method in the interim but should not stand up a new alternative credential infrastructure if one is not already in place.

The General Services Administration, which creates and issues the SmartID cards, established a limit of one identity on each SmartID card and one card per person. However, the policy conflicts with the IRS Cybersecurity office's policy that requires a separate identity to perform administrator services on computer systems. Computer administrators at the IRS are issued two identities, one for end-user access and another for their elevated administrator access.

The conflicting policies and the IIAM project's focus on other project initiatives hindered the IRS from making progress in this crucial area. When the IRS began the RSSO deployment in May 2012, none of the computer administrators had the capability to use their SmartID cards for logical access. The lack of progress is significant because administrator accounts have the most elevated privileges on computer systems. Unauthorized access to these accounts could allow malicious users to cause significant damage and disruption.

Inadequate progress has been made to enable the use of SmartID cards for authentication to applications

IRS employees access approximately 1,900 internal applications. However, the IRS informed us that only 12 applications have been enabled to use a PIV authentication service. The term "PIV-enabled" refers to an application authenticating a user with the credentials on the user's SmartID card and a personal identification number, without requiring the user to type in a password. The Oracle ESSO software does not meet the above requirement because it simply remembers and automatically provides the password to some applications. The Oracle ESSO software does not reduce use of passwords to authenticate to the applications. Furthermore, the Oracle ESSO does not reduce the number of identity stores, which is a key security goal of PIV-enabling applications.

To meet the Department of Homeland Security's directive to expedite the use of SmartID cards for logical access, the Treasury Department[9] defined its interpretation of this requirement as it relates to accessing applications.

[8] Identity, Credential, and Access Management Subcommittee, *Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guide* (Ver. 2) (Dec. 2011); issued under the auspices of the Federal Chief Information Officers Council and at the request of the Federal Enterprise Architecture.
[9] Department of the Treasury, *Department of the Treasury Interpretation on Personal Identity Verification Enablement of Logical Access Control Systems* (Nov. 2011).

> *The Department considers an application to be PIV-enabled if: it directly validates the user's PIV Authentication Certificate; or relies upon a PIV-enabled authentication service. To enhance the usability of our PIV-enabled applications, the Department is pursuing industry standard role-based access control systems that leverage PIV authentication such as Integrated Windows Authentication (IWA), CA Site Minder, and others.*

The lack of progress is due to the Internal Identity and Access Management program delaying this work until Phase 3 of the program. Program officials also cited a lack of resources to change the existing applications. This has prevented the IRS from reducing the number of identity stores that are used by the applications. The greater number of identity stores increases the length of time it takes system administrators to remove access for terminated users. This issue increases the risk of unauthorized access to the applications.

Inadequate progress has been made to configure the Enterprise Remote Access Project to use SmartID Cards

The IIAM project has not made adequate progress to modify the Enterprise Remote Access Project, the IRS virtual private network, to use the SmartID cards for authentication. The virtual private network provides employees throughout the organization the capability to remotely log in to the network and access information technology resources such as e-mail and applications. Employees use the virtual private network while working in remote locations such as the employee's home, a taxpayer's office, or a hotel.

Although developing SmartID card authentication for the virtual private network is required in the IIAM project's tailoring plan, the IRS does not plan to begin deploying a solution until the summer of 2012. Furthermore, the project team does not know when the effort will be completed or why this part of the project is delayed.

The lack of progress will result in employees using their passwords and grid cards to authenticate to the virtual private network for an indefinite period. Although grid cards are a form of two-factor authentication, this method is less secure and violates the mandate to use the SmartID cards for two-factor authentication.

Recommendations

Recommendation 1: Subsequent to completing security testing for the two-factor authentication system, the Chief Technology Officer should direct IRS Labor Relations to notify the National Treasury Employees Union and begin negotiating mandatory use of the SmartID cards.

> **Management's Response:** The IRS agreed with this recommendation and stated the solution is deployed as a component that is integrated into existing systems, and those systems are evaluated in accordance with Cybersecurity policy. The Office of Labor

Strategy and Negotiations will issue notice to the National Treasury Employees Union and bargain as appropriate once the IRS has advised it that the processes and procedures for two-factor authentication with consideration for misplaced or inoperative cards is ready for implementation. The IRS also responded that security testing is not a condition for mandatory use of the SmartID cards.

Office of Audit Comment: We disagree with the IRS's statement that security testing is not a condition for mandatory use of the SmartID cards. The IRS's Security Assessment and Authorization procedures require security testing when a significant change is made to a major system. The IRS defined the RSSO as a major change and the General Support System 32, which houses the RSSO components, is a major system. The IRS should conduct the required security testing prior to requiring employees to use the SmartID cards.

Recommendation 2: The Assistant Chief Information Officer, Cybersecurity, should appoint a certified project manager with the requisite training and experience to lead the IIAM project and provide sufficient full-time staffing and resources to the IIAM project.

Management's Response: The IRS agreed with the spirit and intent of this recommendation. The IRS will appoint a qualified project manager and will provide the necessary project resources to the IIAM project as documented in the IT Integrated Release Plan.

Recommendation 3: The Assistant Chief Information Officer, Cybersecurity, should direct the IIAM project manager to select the most feasible method to implement two-factor authentication for administrators and coordinate the activities needed to implement the interim and long-term solutions.

Management's Response: The IRS agreed with this recommendation. By July 2014, the Associate Chief Information Officer, Cybersecurity, will assign project resources to determine if a viable solution for administrators using the SmartID card exists. If no viable solution exists, the IRS will direct project resources to develop and implement alternatives for an interim solution until a viable solution can be implemented.

Office of Audit Comment: The July 2014 completion date set by the IRS is not timely. In its February 2011 memorandum, the Department of Homeland Security required agencies to expedite the use of the SmartID cards for logical access and upgrade existing logical access control systems to use the SmartID cards prior to using development and technology funds to complete other activities. The IRS should prioritize the efforts to implement two-factor authentication for administrators and set an earlier completion date for its corrective actions.

Recommendation 4: The Assistant Chief Information Officer, Cybersecurity, should direct the IIAM project manager to prioritize and coordinate the work to establish the infrastructure needed to PIV-enable applications.

Management's Response: The IRS agreed with this recommendation. The IRS believes its current implementation, along with the work done to Active Directory, would meet the Treasury Department definition of PIV-enabled infrastructure/applications. The IRS will develop a plan to prioritize and coordinate the remaining work to establish the infrastructure needed for PIV-enabled applications.

Office of Audit Comment: Developing a plan to implement this recommendation is not sufficient. The IRS should place a higher priority on PIV-enabling IRS applications and reducing the number of identity stores used by the applications.

Recommendation 5: The Assistant Chief Information Officer, Cybersecurity, should direct the IIAM project manager to coordinate and lead the activities to plan, develop, test, and deploy two-factor authentication using SmartID cards for logical access to the Enterprise Remote Access Project.

Management's Response: The IRS agreed with this recommendation. A solution for remote access using the SmartID cards was developed and tested. Based on this testing, the User and Network Services function is upgrading components of the network infrastructure that are required to support the use of the SmartID cards for remote access. The IRS set an October 2014 completion date for this recommendation.

Office of Audit Comment: We believe that October 2014 is not a timely deadline to provide SmartID card authentication for employees working remotely. The IRS should make its corrective actions a higher priority and set an earlier completion date.

Required Testing Was Not Conducted

The project team deployed the RSSO without performing the required testing to determine if the system is secure and functions as intended.

Security testing was not conducted

The IIAM project team waived the Security Assessment and Authorization requirement in October 2009 based on advice from the Cybersecurity office. The Cybersecurity office advised the project team that it could bypass the Security Assessment and Authorization process because the process is not applicable to a commercial off-the-shelf software implementation as long as the software is part of the IRS Enterprise Architecture. However, as presented in Appendix IV, the two-factor authentication system includes several components in addition to the software.

At the end of our fieldwork, the IRS informed us it would perform an event-driven security control assessment to assess the security controls in place for the RSSO and to help determine if the system is appropriately safeguarded. However, security testing should have been conducted prior to system deployment to provide assurance that security risks and vulnerabilities are identified and mitigated.

Other types of required testing were also not conducted

The End of Test Completion report is a crucial ELC artifact that is required to summarize the actual testing results and identify the test approach, design, planning, and execution variances from the original test plan. The report should also provide the conclusions and recommendations for the project as a whole. These results should then be considered by the Security Services and Privacy Executive Steering Committee. The End of Test Completion report should address the following types of testing:

- **Integration** – The purpose of integration testing is to verify functional, performance, and reliability requirements placed on major design items. Test cases are constructed to test that all components interact.
- **Application** – Application testing deals with tests for the entire application. This is driven by the scenarios from the analysis team. Application limits and features are tested. The application must successfully execute all scenarios before it is ready for general use.
- **Infrastructure** – Infrastructure testing helps determine how well the network and infrastructure cope with change, specifically in relation to performance, availability, security, and scalability.
- **Capacity** – Capacity testing occurs when you simulate a surge in the number of users, stressing an application's hardware infrastructure.
- **Performance** – Performance testing is an assessment that requires an examinee to actually perform a task or activity, rather than simply answering questions referring to specific parts. The purpose is to ensure greater fidelity to what is being tested.

The integration, infrastructure, capacity, and performance testing for the RSSO were not addressed in the End of Test Completion report, and we found no evidence this testing was conducted. The system to authenticate employees to the network using their SmartID cards was not tested.

Several sections of the End of Test Completion report were missing, such as the detailed test results and defect summary sections. Other sections, such as the executive summary and conclusions and recommendations, contained default wording from the template, indicating the report was not tailored to the IIAM project. In addition, the report was not approved by the required officials, such as the preparer, project lead, test program office coach, senior test specialist, and test program office manager.

The improper waiving of testing and deficiencies in the End of Test Completion report are due to inadequate project oversight and the Cybersecurity office's opinion that the RSSO was merely a commercial off-the-shelf software implementation. The IIAM project team also cited the successful pilot that ended in March 2010 as justification for not conducting the testing. However, the pilot was conducted primarily to test the ActivClient middleware and the

Passlogix v-GO SSO software. Users were given the option of using their SmartID cards to authenticate to the network, but we saw no evidence this authentication system was tested.

Testing was also conducted after the pilot, from December 2011 to May 2012, but this testing focused only on employees installing the Oracle ESSO software on their workstations and using their SmartID cards to access and use of the Oracle ESSO software. This post-pilot testing by 24 employees did not include testing to evaluate the use of SmartID cards to authenticate to the network.

Without performing the required testing, the IRS does not have adequate assurance that the system will operate as intended and that risks have been identified and mitigated.

Key Enterprise Life Cycle Artifacts and Processes Were Not Completed

All IRS projects are required to follow the ELC. The ELC is the approach used to manage and implement business change through information systems initiatives, and it provides the artifacts and processes needed to accomplish business change in a consistent and repeatable manner. The overall objective of the ELC is to enhance chances for success by reducing risk and ensuring compliance with internal and external standards and mandates.

Two key artifacts were not completed and two artifacts were improperly waived

System Deployment Plan – The System Deployment Plan is required to define the detailed set of deployment activities that must be completed to deploy the IIAM components into the operating environment. It should include the dependencies, roles and responsibilities, and deployment schedule. However, these details were not included in this artifact. The required comprehensive list of deployment activities and the start and end dates for the activities were missing. The System Deployment Plan included details only for the pilot and was not updated after the pilot was completed. An example of a crucial missing activity is the communication packet that must be sent to employees. The communication packet advises employees on how to install the software and what to do in the event of technical difficulties; it also contains the security policies regarding the new two-factor authentication system. These details were not included in the System Deployment Plan. In addition, five of the six officials required to review and approve this artifact did not sign the document.

Transition Management Plan – The Transition Management Plan should provide the activities to ensure a smooth transition from the developing to the receiving organization that will maintain and support the new system. Readiness assessment workshops must be conducted, and the results should be documented in the Transition Management Plan.

The following questions should be answered in this artifact.

1. How are business processes and procedures impacted?
2. Will you have enough staff when the system is delivered?
3. Does your staff need additional skills?

We found no evidence that the readiness assessment workshops were conducted, and the Transition Management Plan lacked the required details. In addition, the document contained forward-looking statements, indicating it was not updated after the Design (Milestone 3) phase. Examples include "The SmartID card usage transition impact to the IRS receiving organization will be assessed in Milestone 4b" and "Cross organization gaps will be updated for any readiness gaps that may be uncovered during the readiness assessment workshops."

In addition to the improper completion of the System Deployment Plan and Transition Management Plan, the project team improperly waived two artifacts, the Functional Configuration Audit and the Physical Configuration Audit.

Functional Configuration Audit – The Functional Configuration Audit is required to evaluate the developed system to determine how well the requirements have been met. The activities include:

- Witnessing test execution or examining the test report to ensure the system functionality matches its requirements.
- Verifying the accuracy of the Requirements Traceability Matrix.
- Tracing the baselined requirements to test cases.

Physical Configuration Audit – The Physical Configuration Audit is required to evaluate the technical documentation against the system, as built, to confirm the documentation's effectiveness for maintenance, support, and operation.

The project team waived the Functional Configuration Audit and Physical Configuration Audit artifacts and documented this risk in the Item Tracking Reporting and Change Control System, justifying the decision as a low risk. The project team also justified its decision by citing the completion of the RSSO pilot. However, as previously stated in this report, the pilot ended in March 2010, more than two years prior to deployment of the RSSO, and did not require employees to log in to the IRS network using the SmartID cards.

The improper completion and waiver of the artifacts is due to the IRS not appointing a project manager with the requisite training and experience to oversee and manage the numerous and complex IIAM project activities. The effects could be felt over the next two years as the IRS attempts to deploy, maintain, and support the two-factor authentication system. The inadequate System Deployment Plan could affect deployment and cause further delays. The inadequate Transition Management Plan could prevent a smooth transition to the receiving organizations

responsible for maintaining and supporting the new two-factor authentication processes. Lastly, by not completing the Functional Configuration Audit and the Physical Configuration Audit artifacts, the IRS does not have adequate assurance that the two-factor authentication system meets all the requirements and will operate as intended when employees begin using their SmartID cards to access the network, applications, and virtual private network.

Some key processes in the Milestone Readiness Reviews were not properly conducted

The Milestone Readiness Review (MRR) is a significant ELC process to determine if the project is in compliance with ELC requirements and ready to begin the next phase of work. The reviewing organization makes a recommendation to the project's Executive Steering Committee on whether the project should be allowed to exit its current milestone and advance to the next phase of work. For the IIAM project, the ELC coach conducted the MRRs. The MRR process requires the coach to verify that process owners and stakeholders approved the artifacts listed in the project's tailoring plan. This process is crucial because the ELC coach does not have the technical expertise to review the artifacts. The ELC coach is also required to validate that the project team conducted the in-depth ELC reviews, such as the Customer Technical Reviews and Life Cycle Stage Reviews, that are listed in the tailoring plan. To perform this process, the ELC coach must again rely on the process owners and stakeholders to conduct these in-depth reviews and raise concerns. The ELC coach should raise concerns if the artifacts are not approved or the in-depth reviews are not conducted.

Key artifacts were not approved by the required officials

The Business System Requirements Report, Business System Concept Report, and Business System Architecture Report are key artifacts required to be completed in the Domain Architecture (Milestone 2) phase of the project. However, these artifacts were not approved by the required officials, each contained proposed comments and changes that were not addressed, and the ELC coach did not raise a concern during the MRR. Examples include:

- The Business System Requirements Report was not approved by the HSPD-12 Program Manager or the Requirements and Demand Management Program Manager. Edits were proposed to the capability requirements section, but the project team did not address them. The capability requirements are the highest level requirements associated with the project.
- The Business System Concept Report was missing the same approvals as the Business System Requirements Report. Comments were made about the key factors that will contribute to the overall success of the project. However, these comments were not addressed in the document.
- The Business System Architecture Report was missing approvals by the: 1) Internal Identity and Access Management Chief Architect, 2) HSPD-12 Program Manager, and

3) Executive Director of Enterprise Architecture. Changes were proposed to the privacy requirements section but were not accepted or addressed by the project team.

During the Design (Milestone 3) phase of the project, the Design Specification Report also lacked the required signatures of the three approving officials. This artifact also contained comments that were not addressed by the project team. Examples include comments and edits to the assumptions and constraints of the project and the business processes.

The ELC coach informed us that he saw the required approvals in e-mail messages but in Calendar Year 2009, it was difficult to get approving officials to electronically sign/approve the artifacts. However, we did not see the required approvals for these documents.

We believe these key artifacts were not properly completed and approved, and the MRR process to detect this deficiency was not effective. When key artifacts are not properly completed and approved, the success of the project is jeopardized. Specifically, the system might not operate as intended and additional delays or problems with the deployment could surface.

The Customer Technical Review and Life Cycle Stage Review for the Integration Test and Evaluation were not conducted

The Integration Test and Evaluation is a significant artifact required in the IIAM project's System Development (Milestone 4b) phase. The purpose of the artifact is to combine all individually developed components into a fully tested release and ensure applicable system tests are completed. The ELC tailoring plan for the project requires an in-depth be performed on the Integration Test and Evaluation. However, this artifact was not completed, the in-depth reviews were not performed, and the ELC coach did not raise a concern during the MRR.

The ELC coach did not take exception to the lack of a Customer Technical Review or a Life Cycle Stage Review and recommended the project be approved to exit its Milestone 4b phase. He stated that a Customer Technical Review was not required to exit Milestone 4b and a Life Cycle Stage Review is recommended but not always required. We disagree and believe the IIAM project team should have completed these in-depth reviews that are required by the project's tailoring plan.

By not verifying project artifacts were approved and validating that all the required reviews were performed, the project was allowed to exit milestones without completing the required work. The IRS does not have adequate assurance that the two-factor authentication system will operate as intended when employees attempt to use their SmartID cards to access the IRS's network and applications. Undetected security vulnerabilities may also surface once the IRS begins to roll out two-factor authentication to employees.

Recommendations

Recommendation 6: To ensure security risks and vulnerabilities are identified and mitigated, the Chief Technology Officer should direct the Cybersecurity organization to ensure the event-driven security control assessment for the General Support System 32 is completed by December 30, 2012.

> ***Management's Response:*** The IRS agreed with this recommendation. The Associate Chief Information Officer, Cybersecurity, will ensure an event-driven security control assessment is performed by December 30, 2012.

Recommendation 7: The Associate Chief Information Officer, Cybersecurity, should direct the project manager to coordinate with the Applications Development Enterprise Systems Testing staff to ensure all required testing is completed, complete the End of Test Completion report, and present the test results to the Security Services and Privacy Executive Steering Committee by December 30, 2012.

> ***Management's Response:*** The IRS disagreed with this recommendation and stated that testing was completed in accordance with guidance established by the ELC Project Management Office. The IRS stated that the RSSO was deployed to users in 2010 to provide feedback to the project team on any operational issues. In addition, the RSSO deployment to all IRS employees is already underway, with approximately 13,000 users already activated. The IRS also stated that additional testing is not necessary and the deployment status and results will be shared with the Security Services and Privacy Executive Steering Committee.
>
> ***Office of Audit Comment:*** Our audit tests determined that the Oracle ESSO software was tested, but the more significant part of the RSSO, which is the capability that will allow employees to use SmartID cards to authenticate to the IRS network, was not tested. We examined pilot test data provided by the IIAM project team as well as all testing documented within the End of Testing Completion Report but could not find evidence that security, integration, capacity, or performance testing was conducted for this crucial part of the RSSO.

Recommendation 8: To ensure MRRs are properly completed, the Associate Chief Information Officer, Strategy and Planning, should direct the ELC office to validate that required ELC reviews such as Customer Technical Reviews and Life Cycle Stage Reviews are properly conducted and all artifacts are finalized and approved by the required officials listed within the artifacts.

> ***Management's Response:*** The IRS agreed with this recommendation and stated the ELC Office should validate that the required ELC reviews, such as the Customer Technical Reviews and the Life Cycle Stage Reviews, are properly conducted following the procedures. The IRS also agreed that the ELC Office should ensure that all the

signatures designated in the artifact's template are provided. Lastly, the IRS stated it is currently updating the above ELC procedures to strengthen and clarify responsibilities.

Recommendation 9: The Associate Chief Information Officer, Cybersecurity, should direct the project manager to conduct the: 1) Functional Configuration Audit, 2) Physical Configuration Audit, and 3) Life Cycle Stage Review for the Integration Test and Evaluation.

Management's Response: The IRS disagreed with this recommendation. The IRS stated that the deployment of RSSO is already underway, with approximately 13,000 users already activated; therefore, additional efforts related to preparing for the Integration Test and Evaluation are not needed. The IRS stated that testing was completed as established by the ELC Program Management Office.

Office of Audit Comment: The IRS did not conduct the required testing for the most significant part of the RSSO, which is the new system employees will use with their SmartID cards to authenticate to the IRS network. The Integration Test and Evaluation is a significant ELC artifact that should be completed to ensure all applicable system tests were conducted. The Functional Configuration audit was also required to be completed to evaluate the developed system and determine how well the requirements have been met. Lastly, the Physical Configuration Audit was required to be completed to evaluate the technical documentation against the system, as built, to confirm the documentation's effectiveness for maintenance, support, and operation.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to evaluate the implementation and security of the IRS's two-factor authentication for logical access.[1] To accomplish our objective, we:

I. Assessed the IRS's implementation of the SmartID two-factor authentication system for logical access to evaluate the progress and determine whether the system meets required security standards.

A. Reviewed the Treasury Department's HSPD-12 implementation policy to determine whether it meets the standards specified by the Department of Homeland Security and whether IRS implementation efforts related to logical access align with the policy. The policy was required to be developed and issued by March 31, 2011.

B. Determined if the two-factor logical access system is secure.

1. Evaluated policies, procedures, and security documentation related to the security of the SmartID card logical access authentication to identify required security controls.

2. Obtained and reviewed Security Assessment and Authorization documentation for the General Support System that hosts the SmartID card two-factor authentication for logical access to determine if two-factor authentication was adequately addressed. (Security Assessment and Authorization was performed for the General Support System but not for the SmartID card two-factor authentication for logical access.)

3. Interviewed the infrastructure engineer who designed the process for logical access authentication to determine the design and security controls that are planned for two-factor authentication.

4. Validated and assessed any security vulnerabilities identified in Steps 1–3.

5. Determined whether the serial numbers for SmartID card certificates, which are passed by the Bureau of the Public Debt's Certificate Authority server to the IRS authentication server, should be encrypted.

[1] See Appendix VII for a glossary of terms used throughout this report.

C. Determined whether the two-factor authentication for logical access is working as intended and identified the cause and effect of delays.

1. Determined the number of employees who are currently using the SmartID cards for logical access and the schedule for full implementation.

2. Determined the number of logical access systems (legacy and modernized systems) that have been upgraded to use the SmartID cards in accordance with National Institute of Standards and Technology guidelines and reviewed the upgrade schedule for noncompliant systems. (For modernized systems, we determined whether the Accounts Management Services system and the Modernized e-File system have been upgraded.)

3. Interviewed IIAM project leaders or appropriate officials to determine if the two-factor authentication for logical access is working as intended and includes key Federal Information Processing Standard requirements and components.

4. Analyzed the deployment plan for the SmartID cards to identify the time period for using SmartID cards for logical access, and determined whether the time period has been rebaselined.

5. Determined when stakeholders were initially involved in the IIAM project by interviewing IIAM members and reviewing ELC Milestone 1 deliverables and processes such as the Project Kickoff meeting, Life Cycle Stage Reviews, and MRRs. We reviewed documentation that shows when and how often the key stakeholders were engaged in the project.

6. Reviewed the System Deployment Plan to determine the activities that should have been completed to mitigate the delays and avoid wasted resources.

7. Determined whether software licenses, infrastructure, electronic certificates, or contractor services acquired for the full deployment of SmartID card usage in Calendar Year 2010 resulted in wasted funds.

II. Determined whether key ELC processes and deliverables were followed and completed for the SmartID card two-factor authentication project and whether any deviations resulted in delays or inefficient use of resources.

A. Determined the ELC path the SmartID card for logical access project followed and whether the project team completed the required key deliverables, processes, and Milestone Exit Reviews through the current milestone.

B. Obtained and analyzed testing documentation for the SmartID card two-factor authentication initiative to determine if security testing is sufficient.

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 Federal Information Processing Standard 201[2] and related Internal Revenue Manual guidelines and the processes followed by the IRS to implement SmartID card use for computer access. We evaluated these controls by conducting interviews and meetings with management and staff, observing operations analysts on site, and reviewing documentation such as standard operating procedures.

[2] National Institute of Standards and Technology, FIPS PUB 201-1, *Federal Information Processing Standards Publication: Personal Identity Verification of Federal Employees and Contractors* (Mar. 2006).

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
Cari D. Fogle, Lead Auditor
Charles O. Ekunwe, Senior Auditor
Bret Hunter, Senior Auditor
Samuel C. Mettauer, Information Technology Specialist
Daniel Oakley, Information Technology Specialist

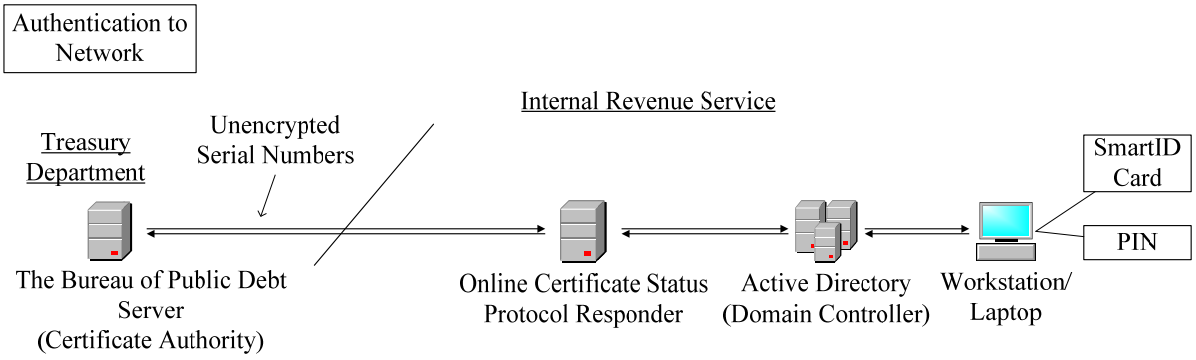
Appendix III

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
Director, Office of Research, Analysis and Statistics RAS
Chief, Criminal Investigations SE:CI
Director, Statistics of Income RAS:S
Human Capital Officer OS:HC
Associate Chief Information Officer, Cybersecurity OS:CTO:C
Associate Chief Information Officer, Enterprise Operations OS:CTO:EO
Associate Chief Information Officer, Enterprise Services OS:CTO:ES
Associate Chief Information Officer, Strategy and Planning OS:CTO:SP
Associate Chief Information Officer, User and Network Services OS:CTO:UNS
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

Authentication to Network Diagram



Authentication to Internal Revenue Service Network

1 – ActivClient is installed on the workstation and required for authentication to the network.

2 – To access the IRS's network, users must use their SmartID card and their personal identification number (PIN).

3 – User name must be a valid name stored on the Domain Controller. User must also enter the correct PIN. After entering a valid PIN, the workstation checks the expiration date on the SmartID card to make sure it is still valid; next it verifies that encryption used on the card matches with the IRS policy.

4 – Users must **not** be on the Validation Proof List. List checks for invalid cards (by serial number) and valid certificates. Lists are replicated from the Bureau of Public Debt to the IRS to decrease traffic flow and to increase efficiency.

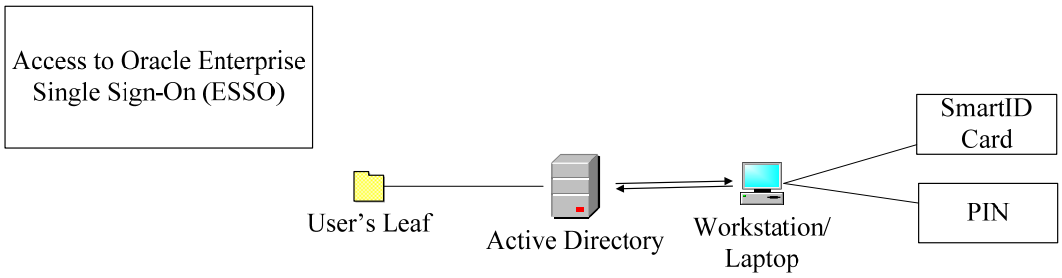
5 – If a user has a valid serial number, certificate, user name, and PIN, the user is authenticated to the network.

Source: Interviews conducted and documents reviewed by the Treasury Inspector General for Tax Administration.

.

Appendix V

Diagram of Oracle Enterprise Single Sign-On Manager Software



Notes for Diagram of Oracle ESSO

1 – To access the Oracle ESSO software, users must insert their SmartID card and their personal identification number.

2 – The Oracle ESSO software is an application installed on a workstation. It enables users to store credentials (user name/password) for applications within their Active Directory leaf. Each user has his or her own leaf.

3 – Users must have a valid card and personal identification number to access the Oracle ESSO software.

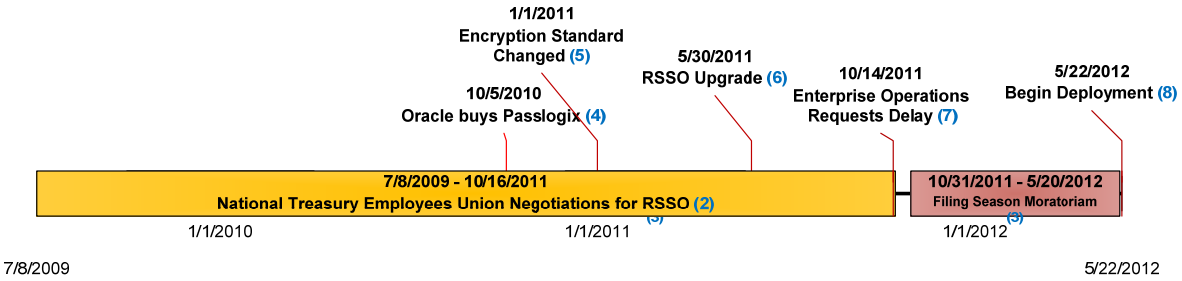
4 – While the SmartID card and personal identification number are used to access the Oracle ESSO software, it is a different process than authenticating to the network. It does not require communication with the Bureau of Public Debt.

5 – The Oracle ESSO software is verifying that the SmartID card and the personal identification number are accurate.

Source: Interviews conducted and documents reviewed by the Treasury Inspector General for Tax Administration.

Appendix VI

Delays in Implementing Reduced SmartID Sign-On (RSSO)



(1) The RSSO pilot was completed in March 2010 with the goal of determining whether Passlogix V-go was appropriate for the entire IRS.

(2) The National Treasury Employees Union negotiated the terms of the RSSO project with the IRS; however, mandating the use of SmartID cards was not negotiated.

(3) Filing season moratoriums would not allow the IRS to deploy the RSSO during the filing seasons.

(4) The Oracle Corporation bought Passlogix, which required the IRS to change the branding of the Passlogix V-go software to The Oracle Corporation and caused delays.

(5) The National Institute of Standards and Technology changed the encryption standards that must be used for the certificates on the SmartID cards.

(6) The Oracle Corporation upgraded the software, which caused additional delays.

(7) The IRS Information Technology organization's Enterprise Operations function requested that the IIAM project not deploy RSSO until the third quarter 2012 because Enterprise Operations released CADE 2 during the filing season and needed to be available in the event CADE 2 had unforeseen issues.

(8) Deployment of the RSSO begins to all laptops and workstations on May 22, 2012.

Source: Interviews conducted and documents reviewed by the Treasury Inspector General for Tax Administration.

Appendix VII

Glossary of Terms

Term	Definition
ActivClient	A commercial off-the-shelf product sold by the ActivIdentity Company that allows workstations to read a user's SmartID card for authentication.
Active Directory Leaf	Active Directory provides a central location for network administration and security. It authenticates and authorizes all users and computers in a Windows network. The leaf object stores users' data.
Administrator Account	An account that has elevated privileges used for managing the system.
Artifact	An artifact is the tangible result of an activity or task performed during the life cycle of a project. There are different categories of artifacts: solution artifacts and management artifacts.
Authentication	The process in which users are granted access to a system based on their identity.
Business System Architecture Report	Documents components of the solution, architecture of how the components fit together and interact, and the plan for implementing the solution over time in the business area.
Business System Concept Report	Documents the future vision for the business area and a conceptual system solution to support the vision.
Business System Requirement Report	Documents all the requirements for the solution.
CA Site Minder	A web access management product that ties security together and offers single sign-on, the process by which a user logs in only once to a web resource and then is automatically logged in to all related resources.
Calendar Year	The 12-consecutive month period ending on December 31.

Commercial Off-the-Shelf	An adjective that describes software or hardware products that are ready-made and available for sale to the general public.
Configuration Item	Fundamental structural unit of a configuration management system. Examples include individual requirements documents, software, models, and plans. The configuration management system oversees the life of the configuration item through a combination of process and tools by implementing and enabling the fundamental elements of identification, change management, status accounting, and audits. The objective of this system is to avoid the introduction of errors related to lack of testing as well as incompatibilities with other configuration items.
Customer Technical Review	A review performed by stakeholders on a work product, or small group of closely related work products produced by a project team, with the purpose of facilitating approval of the work product by ensuring early stakeholder feedback as well as early identification and resolution of issues and actions.
Design Specification Report	Documents logical design of the data and application perspectives.
Encryption	The process of transforming information (referred to as plaintext) using an algorithm (called a cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.
End of Test Completion Report	Summarizes results of tests conducted, including conditions passed and failed.
Enterprise Architecture	A strategic information asset base which defines the mission, the information and technologies necessary to perform the mission, and the transitional processes for implementing new technologies in response to the changing needs of the mission.
Enterprise Life Cycle (ECL)	A standard approach to manage and implement business change through information systems initiatives. The ELC provides the direction, processes, tools, and assets necessary to accomplish business change in a consistent and repeatable manner.

Event-Driven Control Assessment	The process by which security controls are assessed following changes to an information technology system. An Event-Driven Control Assessment only applies to systems with an existing security authorization. It does not apply to new systems without a security authorization, nor does it apply to systems whose security authorization is expiring. These systems will still follow the current IRS Security Assessment and Authorization process.
Filing Season	The period from January 1 through mid-April when most individual income tax returns are filed.
Fiscal Year	A 12-consecutive-month period ending on the last day of any month, except December. The Federal Government's fiscal year begins on October 1 and ends on September 30.
Functional Configuration Audit	An examination of test documentation and evaluation data to verify that if testing of a developed product is successful, then the product is acceptable (*i.e.*, "good enough"), as determined by the Subject Matter Expert and the witnessing of the testing process or reviewing test results documentation to verify that the configuration item has achieved the functionality specified in the relevant configuration.
General Support System 32	An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people. General System Support 32 relates to IRS workstations and support.
Grid Card	A method of identifying users in which the user is asked to input a series of characters based on a preregistered pattern on a grid (that the user knows) and a grid of pseudo-random characters generated by the authenticator. This method results in a different series of characters each time the user authenticates.
Identity Store	A system that maintains identity information. An identity store is often an authoritative source for some of the information it contains.

Integrated Windows® Authentication	A method of authenticating users to other systems in which Integrated Windows authentication does not initially prompt for a user name and password. The current Windows user information on the client is used for Integrated Windows Authentication.
Integration Test and Evaluation	The purpose is to combine all individually developed components into a fully tested release.
Item Tracking Reporting and Control System	An information tracking system used to track and report on issues and action items in the modernization effort.
Life Cycle Stage Review	Provides a broad, horizontal look across the technical and business aspects of the solution being developed to verify that it is appropriately constituted (*i.e.*, complete, consistent, and correct) given its point in the life cycle and to approve the solution for baselining.
Logical Access	Controls used to determine the electronic information and systems that users and other systems may access and the actions that may be performed to the information accessed.
Middleware	Software that functions at an intermediate layer between applications and operating system or database management system or between client and server.
Milestone Exit Review	One of the features in the Governance Layer of the ELC Framework. Milestone Exit Reviews are project reviews performed by IRS executives when a project has reached a life cycle milestone to determine if the project will be allowed to continue on to the next milestone and, if necessary, to approve the required funding.
Milestone Readiness Review	A project review performed to determine if the project is ready to begin the milestone exit process. Its objectives are to help eliminate last minute project delays and rework often experienced during Milestone Exit Reviews and to streamline decisions made by the project's governance organization. The Milestone Readiness Review uses existing information to determine whether or not the project team has satisfied conditions outlined in the tailoring plan.

National Institute of Standards and Technology	Under the Department of Commerce, this organization is responsible for developing standards and guidelines for providing adequate information security for all Federal Government agency operations and assets.
Operating System	An operating system is a set of software that manages computer hardware resources and provides common services for computer programs. The operating system is a vital component of the system software in a computer system. Application programs require an operating system to function.
Physical Configuration Audit	An examination of the technical documentation for designated configuration items to verify that the technical documentation, such as requirements, drawings, and software code listings, which defines the configuration items conforms to the "As-Built" configuration items.
Requirements Traceability Matrix	A tool showing the relationship between test requirement and test cases.
Scalability	Scalability is the ability of a system, network, or process to handle a growing amount of work in a capable manner or its ability to be enlarged to accommodate that growth.
Secure Hash Algorithm	The Secure Hash Algorithm is one of a number of cryptographic hash functions published by the National Institute of Standards and Technology as a U.S. Federal Information Processing Standard.
Service Patch	A fix to software program. A patch is an actual piece of object code that is inserted into (patched into) an executable program. Patches typically are available as downloads over the Internet.
Subject Matter Expert	A subject matter expert or domain expert is a person who is an expert in a particular area or topic.
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.
System Deployment Plan	Presents the detailed plan for deploying a solution at one or more sites.

Tailoring Plan	Tailoring is modification of standard provisions of the IRS's ELC to meet the unique needs of a specific project. The project tailoring plan documents all tailoring decisions, explains the nature of all modifications, and provides justification for each change. The plan includes initial tailoring performed for the project as a whole as well as tailoring refinements made to address project releases and individual life cycle phases. The published tailoring plan documents the engineering path, work products, and reviews that a project will follow during its development life cycle.
Transition Management Plan	Presents a plan for ensuring post-deployment readiness for affected end-user and operations and maintenance organizations.
Two-Factor Authentication	An approach to authentication which requires the presentation of two or more of the three authentication factors: something the user knows (a personal identification number), something the user has (a SmartID card), and something the user is (a fingerprint).
Virtual Private Network	Technology for using the Internet to connect computers to isolated remote computer networks that would otherwise be inaccessible. A virtual private network provides security so that traffic sent through the virtual private network connection stays isolated from other computers.

Appendix VIII

Management's Response to the Draft Report

CHIEF TECHNOLOGY OFFICER

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

SEP 14 2012

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Terence V. Milholland
Chief Technology Officer

SUBJECT: Draft Audit Report – Using SmartID Cards to Access Computer Systems Is Taking Longer Than Expected (Audit # 201120011) (e-trak # 2012-34859)

Thank you for the opportunity to review your draft audit report and meet with the audit team to discuss the IRS's two-factor authentication system for accessing computer systems. We appreciate your report recognizing that updates to the IRS's implementation policy are consistent with the Treasury Department and Department of Homeland Security directives. In addition, the report recognized that the IRS upgraded the level of encryption for the certificates on the SmartID cards.

The IRS is committed to continuously improving security, increasing government efficiency, reducing identity fraud, and protecting personal privacy. The IRS agrees with the general premise of the report that we have not made sufficient progress on implementation of Smart Cards for logical access. However, the IRS disagrees with continuing any further work related to testing and configuration audits of the Reduced Single Sign On (RSSO) implementation. Testing was completed as established by the Enterprise Life Cycle Project Management Office. In addition, the RSSO implementation is underway with the expected usage of 25,000 IRS users by the end of the year. The attachment to this memo details our planned corrective actions.

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

Attachment

Draft Audit Report – Using SmartID Cards to Access Computer Systems Is Taking Longer Than Expected (Audit # 201120011) (e-trak # 2012-34859)

RECOMMENDATION #1: Subsequent to completing security testing for the two-factor authentication system, the Chief Technology Officer should direct IRS Labor Relations to notify the National Treasury Employees Union and begin negotiating mandatory use of the SmartID cards.

CORRECTIVE ACTION #1: The IRS agrees with this recommendation. The solution is deployed as a component that is integrated into existing systems, and those systems are evaluated in accordance with Cybersecurity policy. Security testing is not a condition for mandatory use as written in this report. The Office of Labor Strategy and Negotiations will issue notice to the National Treasury Employees Union and bargain as appropriate once the IRS has advised that processes and procedures for two-factor authentication with consideration for misplaced or inoperative cards is ready for implementation.

IMPLEMENTATION DATE: July 1, 2013

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: N/A

RECOMMENDATION #2: The Assistant Chief Information Officer, Cybersecurity, should appoint a certified project manager with the requisite training and experience to lead the IIAM project and provide sufficient full-time staffing and resources to the IIAM project.

CORRECTIVE ACTION #2: The IRS agrees with the spirit and intent of this recommendation. The IRS will appoint a qualified project manager and will provide the necessary project resources to the IIAM project as documented in the IT Integrated Release Plan.

IMPLEMENTATION DATE: February 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 and monitor them on a monthly basis until completion.

RECOMMENDATION #3: The Assistant Chief Information Officer, Cybersecurity, should direct the IIAM project manager to select the most feasible method to implement two-factor authentication for administrators and coordinate the activities needed to implement the interim and long-term solutions.

Attachment

Draft Audit Report – Using SmartID Cards to Access Computer Systems Is Taking Longer Than Expected (Audit # 201120011) (e-trak # 2012-34859)

CORRECTIVE ACTION #3: The IRS agrees with this recommendation. The Associate Chief Information Officer, Cybersecurity will assign project resources to determine if a viable solution for administrators using the smart card exists. If no viable solution exists, the IRS will direct project resources to develop and implement alternatives for an interim solution until a viable solution can be implemented.

IMPLEMENTATION DATE: July 1, 2014

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 Assistant Chief Information Officer, Cybersecurity, should direct the IIAM project manager to prioritize and coordinate the work to establish the infrastructure needed to PIV-enable applications.

CORRECTIVE ACTION #4: The IRS agrees with this recommendation. The IRS believes that our current implementation, along with the work done to Active Directory would meet the Treasury definition of PIV enabled infrastructure/applications. The IRS will develop a plan to prioritize and coordinate the remaining work to establish the infrastructure needed to PIV enable applications.

IMPLEMENTATION DATE: July 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 and monitor them on a monthly basis until completion.

RECOMMENDATION #5: The Assistant Chief Information Officer, Cybersecurity, should direct the IIAM project manager to coordinate and lead the activities to plan, develop, test, and deploy two-factor authentication using SmartID cards for logical access to the Enterprise Remote Access Project.

CORRECTIVE ACTION #5: The IRS agrees with this recommendation. A solution for remote access using the cards was developed and tested. Based on that pilot, User

Attachment

Draft Audit Report – Using SmartID Cards to Access Computer Systems Is Taking Longer Than Expected (Audit # 201120011) (e-trak # 2012-34859)

Network Services is upgrading components of the network infrastructure required to support the use of the card for remote access.

IMPLEMENTATION DATE: October 1, 2014

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 #6: To ensure security risks and vulnerabilities are identified and mitigated, the Chief Technology Officer should direct the Cybersecurity organization to ensure the event-driven security control assessment for the General Support System 32 is completed by December 30, 2012.

CORRECTIVE ACTION #6: The IRS agrees with this recommendation. We will ensure an event-driven security control assessment is performed by December 30, 2012.

IMPLEMENTATION DATE: January 2, 2013

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 #7: The Associate Chief Information Officer, Cybersecurity, should direct the project manager to coordinate with the Applications Development Enterprise Systems Testing staff to ensure all required testing is completed, complete the End of Test Completion report, and present the test results to the Security Services and Privacy Executive Steering Committee by December 30, 2012.

CORRECTIVE ACTION #7: The IRS does not agree with this recommendation. Testing was completed in accordance with the guidance established by the Enterprise Life Cycle Project Management Office. Furthermore, Reduced Single Sign On deployed to users in 2010 to provide feedback to the project team on any operational issues. RSSO deployment to all IRS is already underway, with approximately 13,000 users already activated. Additional testing is not necessary. Deployment status and results will be shared with the Security Services and Privacy Executive Steering Committee.

IMPLEMENTATION DATE: N/A

Attachment

Draft Audit Report – Using SmartID Cards to Access Computer Systems Is Taking Longer Than Expected (Audit # 201120011) (e-trak # 2012-34859)

RESPONSIBLE OFFICIAL: N/A

CORRECTIVE ACTION MONITORING PLAN: N/A

RECOMMENDATION #8: To ensure MRRs are properly completed, the Associate Chief Information Officer, Strategy and Planning, should direct the ELC office to validate that required ELC reviews such as Customer Technical Reviews and Life Cycle Stage Reviews are properly conducted and all artifacts are finalized and approved by the required officials listed within the artifacts.

CORRECTIVE ACTION #8: The IRS agrees with this recommendation. The ELC Office should validate that the required ELC reviews, such as the Customer Technical Reviews (CTR) and the Life Cycle Stage Reviews (LCSR), are properly conducted following the procedures. We agree that the ELC Office should ensure that all the signatures designated in the artifact's template are provided.

The ELC Office is currently updating the Milestone Readiness Review (MRR), the CTR, and the LCSR to clarify and strengthen their responsibilities.

IMPLEMENTATION DATE: February 1, 2013

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Strategy & Planning

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 #9: The Associate Chief Information Officer, Cybersecurity, should direct the project manager to conduct the: 1) Functional Configuration Audit, 2) Physical Configuration Audit, and 3) Life Cycle Stage Review for the Integration Test and Evaluation.

CORRECTIVE ACTION #9: The IRS does not agree with this recommendation. Deployment of Reduced SmartID Sign-On is already underway with approximately 13,000 users already activated; therefore, additional efforts related to preparing for the Integration Test and Evaluation are not needed. Testing was completed as established by the ELC PMO.

IMPLEMENTATION DATE: N/A

RESPONSIBLE OFFICIAL: N/A

Attachment

Draft Audit Report – Using SmartID Cards to Access Computer Systems Is Taking Longer Than Expected (Audit # 201120011) (e-trak # 2012-34859)

CORRECTIVE ACTION MONITORING PLAN: N/A