TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

# Progress Has Been Made; However, Significant Work Remains to Achieve Full Implementation of Homeland Security Presidential Directive 12

**September 12, 2014**

**Reference Number: 2014-20-069**

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

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

**PROGRESS HAS BEEN MADE; HOWEVER, SIGNIFICANT WORK REMAINS TO ACHIEVE FULL IMPLEMENTATION OF HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 12**

# Highlights

**Final Report issued on September 12, 2014**

Highlights of Reference Number: 2014-20-069 to the Internal Revenue Service Chief Technology Officer.

## IMPACT ON TAXPAYERS

Issued in August 2004, the Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors,* requires Federal agencies to issue identity credentials that meet the HSPD-12 standard and use them for gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems. Without full implementation of HSPD-12 compliant authentication, IRS facilities, networks, and information systems are at an increased risk of unauthorized access.

## WHY TIGTA DID THE AUDIT

This audit was initiated to determine the IRS's progress in implementing HSPD-12 requirements for accessing IRS facilities and information systems. The U.S. Department of the Treasury has set a goal for its bureaus to achieve 100-percent HSPD-12 compliance by Fiscal Year 2015. In Fiscal Year 2012, the Administration identified HSPD-12 as a Cross-Agency Priority initiative needed to improve the security of Federal data.

## WHAT TIGTA FOUND

The majority of the IRS workforce has been issued HSPD-12 compliant Personal Identity Verification (PIV) cards. However, full implementation of PIV card electronic authentication for accessing IRS facilities is not scheduled until at least Fiscal Year 2018, and only if funding is available. In addition, significant challenges remain in the area of implementing PIV card electronic authentication for accessing IRS networks and information systems. These challenges include many legacy systems and technologies in use at the IRS that are incompatible with PIV cards, and limited HSPD-12 staffing and funding for resolving these conflicts.

## WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Technology Officer and Chief, Agency-Wide Shared Services, ensure that all IRS facilities are equipped with HSPD-12 compliant physical access control systems. Also, TIGTA recommended that the Chief Technology Officer ensure that specific requirements, staffing, and scheduling are identified and adequate funding requested to ensure full implementation of mandatory PIV card access to the IRS network and information systems; issue an IRS-wide memorandum to reiterate the requirement for full PIV card adoption; and ensure that HSPD-12 compliant requirements are integrated in the IRS's lifecycle management process to ensure that new and existing systems implement this requirement.

The IRS agreed with all of our recommendations and has planned appropriate corrective actions to address them. The IRS plans to continue to implement HSPD-12 compliant access control systems at IRS facilities, identify and oversee funding needed to support full implementation of HSPD-12, issue an IRS-wide memorandum reiterating the requirements for full adoption of PIV card access to the IRS network and information systems, and ensure that HSPD-12 requirements are integrated into the IRS's enterprise lifecycle development processes.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 12, 2014

**MEMORANDUM FOR** CHIEF TECHNOLOGY OFFICER

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

**SUBJECT:** Final Audit Report – Progress Has Been Made; However, Significant Work Remains to Achieve Full Implementation of Homeland Security Presidential Directive 12 (Audit # 201420003)

This report presents the results of our review of the Internal Revenue Service's (IRS) progress in implementing Homeland Security Presidential Directive 12 requirements for accessing IRS facilities and information systems. This audit was initiated as part of the Treasury Inspector General for Tax Administration's Fiscal Year 2014 Annual Audit Plan and addresses the major management challenge of Security for Taxpayer Data and Employees.

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

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

# *Table of Contents*

# *Abbreviations*

| | |
|---|---|
| AWSS | Agency-Wide Shared Services |
| FY | Fiscal Year |
| HSPD-12 | Homeland Security Presidential Directive 12 |
| IIAM | Internal Identity and Access Management |
| IRS | Internal Revenue Service |
| OMB | Office of Management and Budget |
| PIN | Personal Identification Number |
| PIV | Personal Identity Verification |
| TIGTA | Treasury Inspector General for Tax Administration |

# Background

On August 27, 2004, President George W. Bush issued Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors,* which requires agencies to follow specific technical standards and business processes for the issuance and routine use of Federal identity credentials.[1] The goal of the initiative is to ensure that only authorized personnel have access to Government systems and applications. This creates a more secure enterprise architecture by reducing the opportunity for identity fraud, thereby increasing the safety of both Government information and personal privacy.

***Personal Identity Verification cards improve security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Governmentwide standard for secure and reliable forms of identification.***

On August 5, 2005, the Office of Management and Budget (OMB) issued policy memorandum M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*, which outlined instructions for implementing HSPD-12. Federal agencies were to issue and require use of identity credentials meeting the HSPD-12 standard for current employees and contractors no later than October 27, 2007, for gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems. It stated that inconsistent agency approaches to facility security and computer security were inefficient and costly, and increased risks to the Federal Government. Successful implementation of the HSPD-12 standard would increase the security of Federal facilities and information systems.

In November 2009, the Federal Chief Information Officers Council released the Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance to aid Federal agencies in implementing HSPD-12. The Federal Identity, Credential, and Access Management Roadmap focused on addressing the challenges and design requirements for Governmentwide identity, credential, and access management, and defining and promoting consistency across the Federal Government. The Federal Government adopted the Personal Identity Verification (PIV) card as the standard identity credential for Federal employees and contractors and as a key element in moving towards strong authentication.[2]

On February 3, 2011, the OMB issued policy memorandum M-11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification*

[1] An identity credential is an object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by an entity.
[2] Authentication is the process of verifying that a claimed identity is genuine and based on valid credentials.

*Standard for Federal Employees and Contractors*, which required each agency to develop and issue an implementation policy through which the agency will require the use of the PIV credentials as the common means of authentication for access to that agency's facilities, networks, and information systems. This memorandum stated that the majority of the Federal workforce was in possession of the PIV credentials and, therefore, agencies should aggressively step up their efforts to use the electronic capabilities of the credentials.

In Fiscal Year (FY) 2012, the Obama Administration identified HSPD-12 as a strategy within the Cybersecurity Cross-Agency Priority Goal. The Cross-Agency Priority Goal strategy is intended to help monitor the implementation of Federal cybersecurity policies and legislation needed to improve the security of Federal data. As part of the Cybersecurity Cross-Agency Priority Goal strategy, the Obama Administration is monitoring the implementation of PIV-card access to Federal information systems. As of the end of FY 2013, the Federal Government as a whole reported to have achieved 67 percent implementation of PIV-card access to Federal information systems. The target set for Federal agencies to achieve by the end of FY 2014 is 75 percent implementation.

The Department of the Treasury (hereafter referred to as the Treasury Department) issued Treasury Directive 71-12 on September 28, 2011, to set policy and define responsibilities for compliance with HSPD-12 with the Treasury Department. The directive required Treasury Department bureaus to plan and report the status of their PIV credential use for physical and logical access to the Treasury Enterprise Identity Credential and Access Management Program Executive Office.

The Internal Revenue Service (IRS) established the Internal Identity and Access Management (IIAM) Program Management Office for achieving the implementation of processes, technologies, and policies to manage user identities throughout their lifecycle, and to meet Federal Identity, Credential, and Access Management and Treasury Enterprise Identity Credential and Access Management goals. Appendix IV presents a graphic depiction of IRS PIV card issuance and use.

The Treasury Inspector General for Tax Administration (TIGTA) has issued the following audit reports on the IRS's efforts to implement the directive. In general, TIGTA reported that progress was slow in implementing HSPD-12 requirements.

- TIGTA, Ref. No. 2007-20-110, *Progress Has Been Slow in Meeting Homeland Security Presidential Directive-12 Requirements* (Jun. 2007).
- TIGTA, Ref. No. 2008-20-030, *Lack of Proper IRS Oversight of the Department of the Treasury HSPD-12 Initiative Resulted in Misuse of Federal Government Resources* (Dec. 2007).
- TIGTA, Ref. No. 2009-20-084, *The Homeland Security Presidential Directive 12 Program Office Has Addressed Prior Weaknesses, but Progress Is Slower Than What Has Been Reported* (Jun. 2009).

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

This review was performed with information obtained from the Information Technology organization's Office of Cybersecurity in Charlotte, North Carolina, and Washington D.C.; and the Agency-Wide Shared Services's (AWSS) Office of Physical Security and Emergency Preparedness in Washington D.C., during the period January through June 2014. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

# Results of Review

The implementation of HSPD-12 is a substantial and complex project at the IRS. The project consists of multiple, interrelated components including implementing interrelated systems for:

- Issuing PIV cards to authorized employees and contractors;
- Using PIV cards to gain physical access to IRS facilities; and
- Using PIV cards to gain logical access to the IRS network and information systems.

The Treasury Department has set a goal for its bureaus to achieve 100-percent HSPD-12 compliance by FY 2015. The IRS has spent more than $110 million[3] to implement HSPD-12 and has budgeted an additional $19 million for FY 2014. Even so, HSPD-12 project management officials cite the lack of sufficient funding and staffing as a main obstacle to completing full implementation of HSPD-12. The majority of the IRS workforce has been issued PIV cards. However, full implementation of physical access controls using PIV card electronic authentication at IRS offices is not scheduled until at least FY 2018, and only if funding is available. In addition, significant challenges remain in the area of implementing logical access controls to IRS networks and information systems using PIV cards. The IRS is not unique in its implementation challenges. Many Federal agencies have experienced challenges in implementing HSPD-12. In March 2013, the OMB reported that not a single Federal agency had fully implemented HSPD-12.

In our September 2012 TIGTA report on HSPD-12,[4] we reported that the IRS had not made adequate progress in areas such as implementing HSPD-12 compliant authentication for system administrators and did not conduct required testing or complete key developmental documents and processes. During this review, we followed up on these issues and found that the IRS had taken action to conduct testing on its HSPD-12 authentication components and complete key project developmental documents. However, the administrator access issue remains one of the technological challenges still impeding the IRS's full implementation of HSPD-12, which we will discuss more fully in the body of our report.

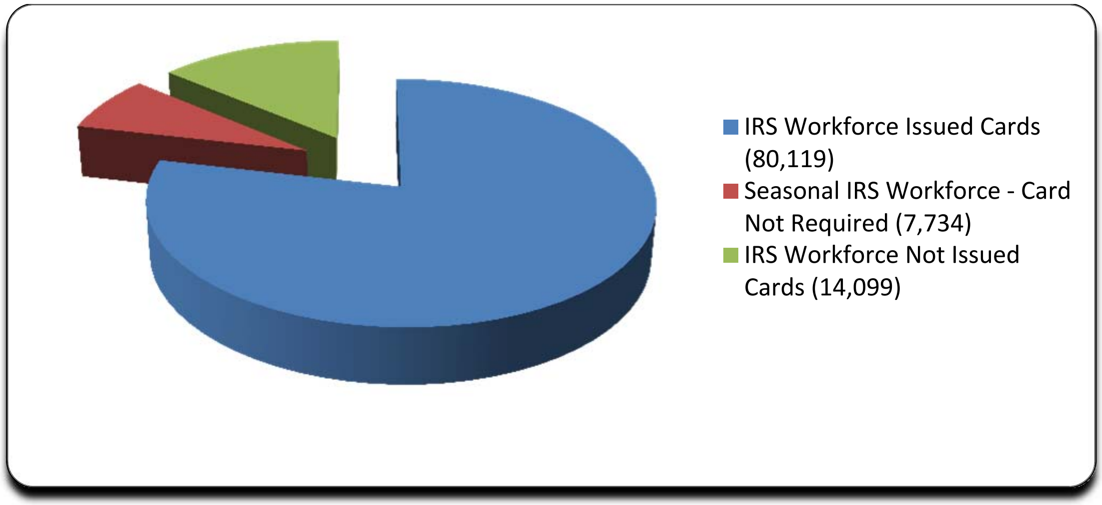
[3] The IRS could not provide us complete cost information that it expended on HSPD-12 implementation for FYs 2005 through 2008; therefore, total implementation cost is likely much higher.
[4] TIGTA, Ref. No. 2012-20-115, *Using SmartID Cards to Access Computer Systems Is Taking Longer Than Expected* (Sept. 2012).

## Personal Identity Verification Cards Have Been Issued to 85 Percent of the Workforce

HSPD-12 requires that agencies issue PIV cards, “to the maximum extent practicable,” to authorized employees and contractors for use in accessing Government offices and information systems. In accordance with OMB M-05-24, Treasury Department policy states that individuals who require physical access to Federally controlled facilities or electronic access to Government information systems for more than six months must be issued a PIV card. The Treasury Department set a goal for its bureaus to sustain their PIV card issuance rates above 90 percent for FYs 2011 through 2015.

The IRS has made steady progress in issuing PIV cards to its employees and contractors. As of February 27, 2014, the IRS’s PIV card database supported that 80,119 PIV cards had been issued, or were in the process of being issued, to IRS network users,[5] achieving an 85 percent issuance rate. The PIV database also listed 14,099 employees and contractors as requiring PIV cards but not yet issued, and 7,734 seasonal employees as not requiring PIV cards. Figure 1 illustrates these figures.

**Figure 1: PIV Card Issuance Implementation Status**

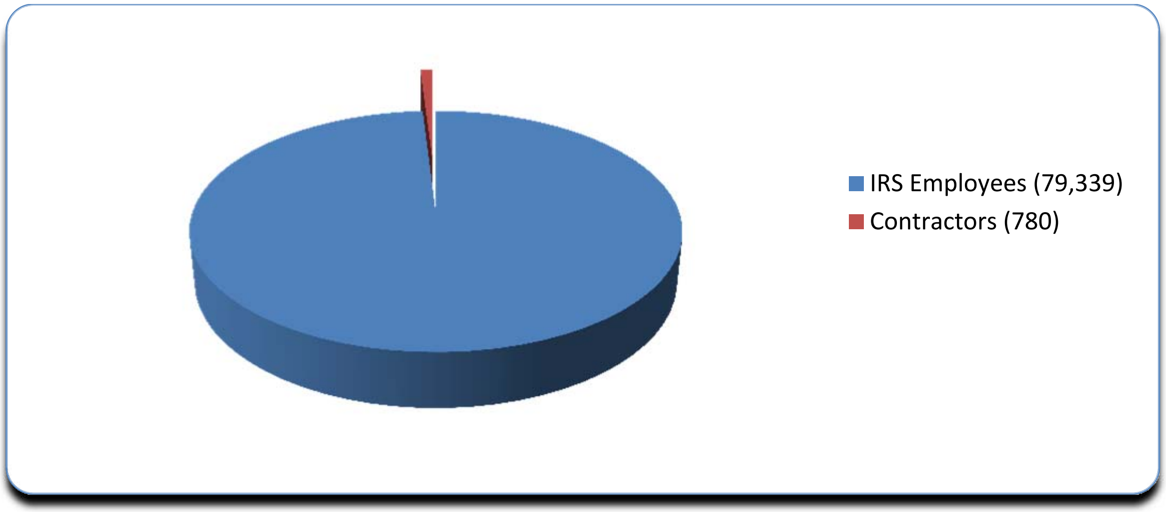


*Source: AWSS database containing PIV card data for IRS employees and contractors.*

Of the 80,119 IRS workforce who have been issued PIV cards, 79,339 are IRS employees and 780 are contractors. Of the 14,099 individuals not yet issued PIV cards, 9,503 are IRS employees and 4,596 are contractors. Figures 2 and 3 illustrate these figures.

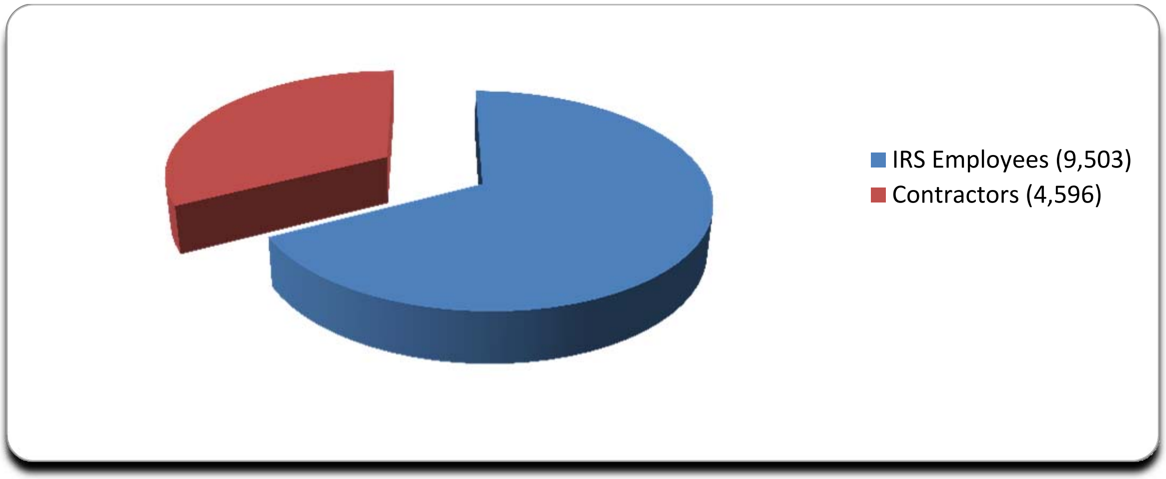
[5] Due to employee turnover, the number of network users fluctuates. For example, from February 14, 2014, to May 30, 2014, the number of networks users declined from 94,951 to 94,251.

### Figure 2: PIV Cards Issued to IRS Employees and Contractors



*Source: AWSS database containing PIV card data for IRS employees and contractors.*

### Figure 3: PIV Cards Not Issued to IRS Employees and Contractors



*Source: AWSS database containing PIV card data for IRS employees and contractors.*

For issued cards, the IRS must perform maintenance activities, such as periodic card and certificate[6] renewals. PIV cards expire every five years and must be renewed. The digital certificate within the card must be rekeyed every three years to keep the certificate up to date and the card operational. As of March 2014, the IRS had renewed more than 58 percent of PIV cards

[6] A certificate is a data object containing a subject identified, a public key, and other information that is digitally signed by a certification authority. Certificates convey trust in the relationship of the subject identifier to the public key. A public key is the public part of an asymmetric key pair that is typically used to verify signatures or encrypt data.

that were expiring during Calendar Year 2014. Also, the IRS had completed certificate rekeys for more than 45 percent of active PIV cardholders for Calendar Year 2014.

However, the IRS has stayed at an 85-percent card issuance rate since FY 2013. Several factors have contributed to the IRS's inability to achieve a higher percentage.

- The IRS's disparate identity environment creates data errors that must be manually corrected. Currently, the provisioning of an IRS identity and issuance of a fully functional PIV card is cumbersome, slow, and includes decentralized manual processes and steps. PIV issuance and population of data attributes for the PIV card involve multiple systems at the IRS, Treasury Department, and Federal levels. The IRS also has multiple internal identity-related systems and processes, owned by the IRS Information Technology organization and the AWSS. These include:

  - Corporate Authoritative Directory Services.
  - Totally Automated Personnel System.
  - Human Capital Office.
  - Career Connector Companion.
  - Human Resources Reporting Center.
  - Online 5081.
  - Active Directory.
  - Active Roles Server and other key systems.

  IRS HSPD-12 project staff indicated that the IRS is currently working missing or mismatched data issues for 5,000 employees and contractors that must be resolved before their PIV cards can be issued. Correcting data errors or mismatches requires a lot of manual research and input from multiple separate data sources at the IRS, Treasury Department, and Federal levels. The Treasury Department periodically runs an exception tool to identify employee and contractor records that are affected by missing data elements that prevent the issuance of the PIV card. AWSS staff must work with the sponsors[7] of these individuals, or must assign a sponsor, to manually correct records and ensure that all the data elements are in place. However, the sponsor's actions may be limited within the various systems, and the AWSS staff often must work with the Treasury Department to make corrections for missing or mismatched data elements.

[7] A sponsor acts on behalf of the agency to facilitate the credentialing process by inputting data elements into authoritative information systems. Depending on the applicant's employment status, a sponsor may be a Federal supervisor, contracting officer, contracting officer's representative, or other Federal official.

- The IRS must manually verify contractor data prior to issuance of PIV cards. Of the 14,099 individuals listed as requiring PIV cards but do not have them yet, 4,596 are contractors. The PIV database provided by the IRS showed that only 780 contractors at the IRS have been issued PIV cards. The IRS must retrieve contractor data needed for PIV card issuance from its PIV Background Investigation Process system. The data from this system must be manually verified to ensure that they are correct, that the contractor is still active, and that the contractor is required to be issued a PIV card. Some contractors listed as needing PIV cards may not in fact need them for various reasons, such as they do not require system access, they work at their own facilities, they are custodial, or they may be employed for less than six months.

- IRS offices at remote locations affect the timely issuance of PIV cards due to their distance from credentialing stations. The IRS has about 65 buildings that are located more than 50 miles from credentialing stations. About 338 employees and contractors located in these offices have not been issued PIV cards. These individuals have been issued legacy identification badges that do not require activation and can be shipped to the employee directly. To be issued a PIV card, these employees must travel to a credentialing station that can issue PIV cards. Therefore, correction of this issue may be affected by budget constraints.

- The IRS's high workforce turnover rate inhibits achieving the PIV card issuance goal. According to AWSS staff, IRS employee records show that its turnover rate has been 12 percent and 13 percent since FY 2009. Therefore, some individuals listed as requiring PIV cards may not be onboard for more than six months due to unexpected/early departures. Also, although seasonal employees that are onboard less than six months do not require a PIV card, sometimes they are inaccurately coded in the system as requiring PIV cards, which causes this number to be inflated.

To resolve the issues related to data consistency and manual processes that have delayed PIV card issuance, the Treasury Department is implementing an enterprise solution, known as PIV Data Synchronization, which will synchronize PIV data across the Treasury Department enterprise, bureaus, and external Federal systems. The PIV Data Synchronization will integrate card issuance with the hiring process and allow issuance of PIV cards to new employees on their first day of work, resulting in the security benefits of immediate PIV access to facilities and information systems for each employee.

In addition, the PIV Data Synchronization will provide a central store for contractors and account for all PIV cards issued to contractors within the Treasury Department. It will reduce redundancy in systems that support contractor access, establish a single repository to account for contractor policy compliance, and serve as a single source for revocation of a contractor's credentials/privileges.

The IRS is in the process of building infrastructure to interface directly with the Treasury Department's PIV Data Synchronization components.[8] The IRS expects that once these systems can interface with each other in real-time, data mismatch problems should largely be resolved, manual processes can be removed, and the secure creation and management of PIV identities will be expedited. The IRS completed the interfaces needed to create IRS employee identities and is working to add the interfaces needed to create contractor identities.

Based on the IRS's ongoing work to improve its identity management and card issuance processes, we are not making any recommendations related to PIV card issuance. The IRS expects its infrastructure improvements will help it meet the HSPD-12 mandate.

## Personal Identity Verification Card Electronic Authentication for Physical Access Has Been Implemented at 21 Percent of Facilities

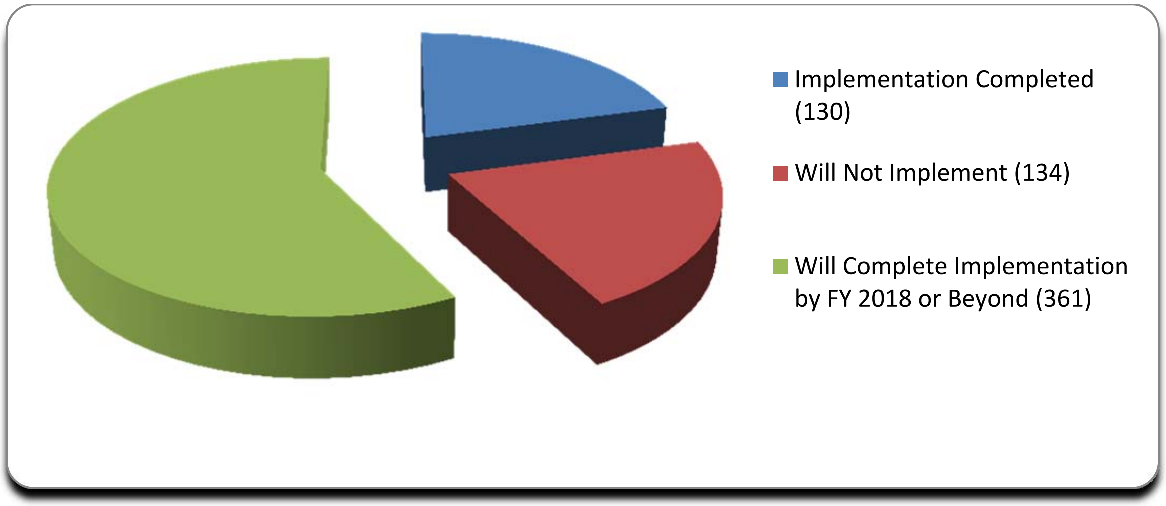
HSPD-12 requires the use of PIV card electronic authentication for physical access to Federal facilities. OMB's October 2005 guidance instructed agencies to use appropriate card authentication mechanisms at their facilities and specified "minimal reliance" on visual authentication as a sole means of authenticating PIV credentials. OMB's February 2011 guidance noted that the majority of the Federal workforce was by then in possession of PIV cards and required agencies to increase usage of the electronic capabilities of PIV credentials as the common means of authentication for access to agency facilities. The Treasury Department set a goal for its bureaus to achieve 100-percent HSPD-12 compliance for physical access by FY 2015.

The IRS has identified 625 locations within the United States and Puerto Rico which require HSPD-12 physical access controls.[9] The IRS has implemented PIV card electronic authentication at 130 (21 percent) of these locations and has determined that it will not upgrade 134 locations for HSPD-12 compliance. The IRS believes the costs of upgrading these locations are not justified because these offices either have a lower security level, or may be consolidated or closed at some future date. Of the remaining 361 facilities, the IRS estimates that it will not complete PIV-based electronic authentication until at least FY 2018, and only if funding is available. Figure 4 illustrates these figures.

[8] The Treasury Department's PIV Data Synchronization components include HR Connect, Data Management Service, Treasury Enterprise Directory Service, and USAccess.

[9] The IRS has employees located at more than 100 additional international offices; however, the State Department is responsible for implementing HSPD-12 physical access controls at these locations.

### Figure 4: Physical Access Controls Implementation Status



*Source: IRS information on implementing PIV card electronic access at IRS facilities.*

The IRS estimates it requires approximately $123 million and an additional six full-time employees to complete implementation at just the 361 offices it intends to make HSPD-12 compliant. Significant additional funding would be required to make compliant the 134 facilities for which the IRS has decided not to make HSPD-12 compliant.

HSPD-12 does not contain provisions for nonimplementation of PIV-based physical access control systems at Federal Government facilities. However, HSPD-12 does suggest that agencies implement PIV-based control systems at higher risk facilities first. Further, the Federal Information Security Management Act of 2002[10] requires all Federal agencies to plan and budget for information technology security. However, the IRS has not budgeted for the full implementation of PIV-compliant physical access to IRS facilities.

Until PIV card authentication for physical access is fully implemented at all IRS offices, the IRS faces an increased risk of unauthorized access at these offices.

## Recommendation

***Recommendation 1:*** The Chief Technology Officer and Chief, Agency-Wide Shared Services, should ensure that all IRS facilities are equipped with HSPD-12 compliant physical access control systems and that the prioritized plans to accomplish this are documented and regularly reviewed for progress. The Chief Technology Officer should consider making HSPD-12 a priority in terms of funding to better allow for its full implementation.

[10] Pub. L. No. 107-347, Title III, 116 Stat. 2899, 2946-2961 (2002) (codified as amended in 44 U.S.C. §§ 3541-3549).

***Management's Response:*** The IRS agreed with this recommendation. The AWSS will continue to install HSPD-12 compliant access control systems at all IRS facilities once the Information Technology organization receives sufficient funding. The AWSS, in conjunction with the Cybersecurity organization, has developed long-range prioritized plans for the installation of compliant, enterprise-wide physical access control systems in the remaining IRS locations that need them. Additionally, joint executive-level and bi-weekly meetings are conducted to review and discuss status updates, resolution of issues, information technology funding availability, and other pertinent matters. The AWSS maintains and frequently reviews the prioritized lists of locations that are still pending physical access control system deployments, and project status is discussed with the Deputy Commissioner of Operations Support during AWSS Business Performance Reviews.

## Personal Identity Verification Card Electronic Authentication for Logical Access to the Network Has Been Implemented for Only 5 Percent of the Workforce

HSPD-12 requires agencies to use PIV cards to access Federal networks and information systems. OMB's 2011 guidance required agencies to step up their efforts to use the electronic capabilities of PIV credentials as the common means of authentication for access to agency information systems. The Treasury Department set a goal for its bureaus to achieve 100-percent HSPD-12 compliance for logical access to networks by FY 2013.

### *Mandatory PIV card authentication to the network has been implemented for only 5 percent of the workforce*

The IRS has implemented mandatory use of PIV cards to access its network for only a small percentage of its network users. As of May 30, 2014, only 5 percent of employees are required to use PIV cards to access the IRS network.

Several challenges have delayed the IRS's progress in meeting the goals set by the Treasury Department for mandatory use of PIV cards to access IRS networks.

- The IRS needed to negotiate a National Treasury Employees Union agreement related to mandatory use of PIV cards prior to its implementation. This agreement was not finalized until July 2013.
- The HSPD-12 project has had limited dedicated resources. Most of the technical staff is temporarily assigned to this project. When the Federal Government shutdown was imminent in September 2013, much of this temporary staff was reassigned to other Information Technology organization functions to administer the shutdown of IRS information technology resources. Similarly, after the shutdown ended, these resources were required to deal with information technology systems restart and the numerous

helpdesk tickets generated from the shutdown and restart of the information technology systems.

- A solution for administrator access to the IRS network and information systems using a single PIV card and Personal Identification Number (PIN) has yet to be identified, tested, and implemented. Based on HSPD-12 requirements, the General Services Administration established a limit of one identity on each PIV card and one card per person. However, to support the security principle of least privilege, Treasury Department policy requires system administrators to have both an end-user account and one or more elevated privileged accounts to allow the system administrator to use an unprivileged account when not performing privileged actions. The requirement that administrators access the Federal networks and applications with a single PIV card and PIN creates a technological challenge across the Federal Government for an individual who needs both administrative and non-administrative type access to networks and information systems. Various solutions have been proposed to the IRS by the Treasury Department's Treasury Enterprise Identity Credential and Access Management group; however, the IRS's testing of these solutions has been designated as low priority due to insufficient funding and resources, as well as its current focus to increase mandatory use of PIV cards for network access, which it sees as a top priority in the progression towards full HSPD-12 implementation. As of May 30, 2014, the IRS reported to have 3,070 people with privileged network accounts.
- The IRS currently has several systems and software which are not HSPD-12 compliant. The HSPD-12 project team provided a list of 25 technologies currently in use at the IRS that users have reported as incompatible with the use of PIV cards, and 18 additional technologies that potentially will cause conflicts. Some examples of these incompatible technologies include: Jabber®, a product by Cisco® that provides instant messaging; pcAnywhere™, a remote control solution by Symantec™ that allows helpdesk staff to access remote computers to resolve issues quickly; Control-M, a product by BMC Software that provides workload automation; and Business Object Enterprise, a product by SAP® that provides reporting and information delivery. The HSPD-12 project team cannot enable mandatory use of PIV cards for the users of the incompatible technologies until solutions to resolve the conflicts are found.

Beginning in April 2014, the HSPD-12 project team embarked on an ambitious implementation schedule where they hope to implement mandatory use of PIV card for access to the IRS network for more than 30,000 additional IRS network users. This effort will bring the total number of network users required to logon with their PIV cards to approximately 35,700 (38 percent of network users) by the end of FY 2014. As technological solutions are developed for incompatible technologies, mandatory PIV card logon will be enabled for additional network users.

## While the IRS has made some progress in updating information systems to accept PIV cards, more work needs to be done

In addition to network access, HSPD-12 requires PIV card authentication to Federal systems and applications. Treasury Department policy requires that all existing systems must be upgraded to use PIV credentials prior to the agency using development and technology refresh funds to complete other activities. Treasury Department policy also requires that new systems under development must be enabled to use PIV credentials prior to being made operational.

The IRS has not implemented PIV card access to most of its existing information systems and applications yet and has conducted limited work in this area. No IRS information systems are exclusively accessed using PIV cards yet. The IRS has many legacy systems that do not work with the PIV card, and a fix must be developed before users can be required to logon with a PIV card. Although the IRS has made recent progress in this area, challenges still exist. For example, the Remittance Transaction Research system was recently updated to support the use of the PIV card. The application itself has about 22,000 users, not all of whom have been issued PIV cards. Therefore, the IRS must continue to allow employees without PIV cards access to this application. While this is progress, more must be done to ensure that all employees are issued cards so that the IRS can enforce the use of PIV cards across all of its infrastructure and application services. Implementing solutions to allow these applications to use the card must be made a priority.

Due to limited staffing and funding, implementing mandatory logon to the IRS network using PIV cards has been a higher priority than implementing PIV card access to all IRS information systems. The IRS's information technology infrastructure has historically been highly decentralized, and systems tend to be implemented at the project or program level. Authentication is implemented, in most cases, on an application-by-application basis. To successfully implement "HSPD 12 compliant" applications utilizing a central authentication source, identity store consolidation and identity data normalization must take place. The HSPD-12 project team has to develop a supporting strategy that clearly articulates how to build the infrastructure needed by application owners to make their applications compliant with National Institute for Standards and Technology guidelines for utilizing PIV credentials. This strategy must also make certain that new infrastructure components are compliant with these guidelines before becoming operational.

The HSPD-12 project team has developed an IIAM Project Management Plan that provides a strategy for building the centralized identity management infrastructure needed to achieve HSPD-12 compliance and meet the Treasury Department's goals and time frames. This plan also identifies challenges that remain in achieving full PIV enablement, including the limited funding and staffing based on the project's prioritization; the long-term approach needed given the size and complexity of the IRS, its business processes, and the critical nature of many of its facilities, systems, and applications; and the current multiple technical environments that frustrate a single-enterprise solution. The plan calls for governance oversight and regular stakeholder communications to discuss and resolve matters that have impact and require coordination IRS-wide. The current plan also calls for the reuse of existing infrastructure components where possible, adding only new components where absolutely necessary. This plan has the potential to accelerate the adoption of the use of PIV cards if given the proper organizational support.

The IRS acknowledges its stewardship responsibilities for ensuring that both agency mission and security objectives are achieved. However, due to constant budget constraints, a key strategy for the IRS Information Technology organization has been to use a risk-based approach towards balancing business results with security requirements in order to continue to provide the core information technology deliverables for achieving mission objectives. However, without full implementation of HSPD-12 compliant authentication services, the IRS network and information systems are at an increased risk of unauthorized access. If funding, staffing, and technical issues are not resolved, full implementation of HSPD-12 compliant authentication will continue to be delayed. In addition, without adequate education and oversight to prevent development or purchase of noncompliant systems or software, full implementation of HSPD-12 will never be achieved.

## Recommendations

The Chief Technology Officer should:

***Recommendation 2:*** Continue to provide oversight and drive implementation of HSPD-12 requirements while balancing resource demands to meet IRS mission objectives. To ensure full implementation of mandatory PIV card access to the IRS network and information systems, specific requirements, staffing, and scheduling should be identified and adequate funding requested to cover those needs, including:

- Specific equipment and support needs should be clearly identified, including hardware and software requirements, testing needs, and any contractor expertise needed.
- Specific staffing needs should be clearly identified to ensure that not only the requisite number of staff is assigned to HSPD-12, but that staff with the correct skills are assigned to the appropriate activities.
- Detailed milestones should be developed and progress on those milestones should be regularly reported to the Chief Technology Officer as part of a detailed plan to implement mandatory logon to IRS networks and information systems with PIV cards and resolve the administrator access issue.

***Management's Response:*** The IRS agreed with this recommendation. The Chief Technology Officer will continue to oversee and identify funding needed to support implementation of the HSPD-12 requirements. To the extent funding is provided, the

Chief Technology Officer will continue with implementation of mandatory PIV card access to the IRS network and information systems as well as:

- Equipment and support;
- Staffing; and
- Development of milestones for full implementation, contingent on funding.

***Recommendation 3:*** Issue an IRS-wide memorandum reiterating the OMB M-11-11 requirement for full adoption of PIV credentials for logical access to the IRS network and information systems.

***Management's Response:*** The IRS agreed with this recommendation. The Chief Technology Officer will issue an IRS-wide memorandum reiterating the IRS's enterprise-wide program to meet the OMB M-11-11 requirement mandating agencies to continue implementation of HSPD-12 policy. The policy is to protect the Nation's infrastructure with the full adoption of PIV credentials for logical access to agency network and information systems.

***Recommendation 4:*** Ensure that HSPD-12 compliant requirements are integrated in the IRS's lifecycle management process to ensure that new and existing systems implement this requirement.

***Management's Response:*** The IRS agreed with this recommendation. The Chief Technology Officer will: 1) notify the Enterprise Services organization to add the use of the PIV as a requirement to all enterprise lifecycle artifacts and solutions development processes, and 2) ensure that the use of the PIV card is fully detailed in the Enterprise Architecture.

## Appendix I

# Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine the IRS's progress in implementing HSPD-12 requirements for accessing IRS facilities and information systems. To accomplish this objective, we:

I. Determined the current status of the IRS's HSPD-12 implementation, and identified issues impeding its full and timely implementation.

   A. Documented and reviewed pertinent HSPD-12 requirements, including the HSPD-12 Directive, OMB memos, National Institute of Standards and Technology publications, Federal Cross-Agency Priority Goals, and summarized requirements and time frames for compliance.

   B. Obtained and reviewed documentation of the most recent IRS goals and implementation status.

   C. Consulted with key IRS personnel regarding the challenges faced relating to implementation and the root causes of those challenges.

II. Followed up on IRS corrective actions pertaining to the September 2012 TIGTA report recommendations.[1]

   A. Determined whether the IRS Labor Relations office completed negotiations with the National Treasury Employees Union on mandatory use of PIV cards.

   B. Determined whether the IRS appointed a project manager to lead the IIAM project and provided sufficient full-time staffing and resources to the IIAM project.

   C. Determined whether the IIAM project manager selected the most feasible method to implement two-factor authentication for administrators and coordinated the activities needed to implement the interim and long-term solutions.

   D. Determined whether the IIAM project manager prioritized and coordinated the work to establish the infrastructure needed to PIV-enable information systems.

   E. Determined whether the IIAM project manager coordinated and led the activities to plan, develop, test, and deploy two-factor authentication using PIV cards for logical access to the Enterprise Remote Access Project.

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

F. Determined whether the Cybersecurity organization ensured that an event-driven security control assessment for the General Support System 32 was completed by December 30, 2012, to ensure that security risks and vulnerabilities were identified and mitigated.

G. Determined whether the project manager coordinated with the Applications Development organization Enterprise Systems Testing function staff to ensure that all required testing was completed and the results presented to the Security Services and Privacy Executive Steering Committee by December 30, 2012.

H. Determined whether the Enterprise Life Cycle office validated that required Enterprise Life Cycle reviews, including Milestone Readiness Reviews, are properly conducted and all required artifacts[2] are finalized and approved by the required officials listed within the artifacts.

I. Determined whether the project manager conducted the: 1) Functional Configuration Audit, 2) Physical Configuration Audit, and 3) Life Cycle Stage Review for the Integration Test and Evaluation.

### ***Internal controls methodology***

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: Federal directives and guidance on HSPD-12, including the HSPD-12 Directive, OMB memos, National Institute of Standards and Technology publications, General Service Administration guidance, Department of the Treasury and IRS policies, and Federal Cross-Agency Priority Goals. We evaluated these controls by reviewing the Federal directives, guidance, and goals related to HSPD-12. We interviewed the IRS IIAM project manager and staff with duties related to HSPD-12. We also obtained and reviewed documentation of the most recent IRS HSDP-12 goals and implementation status.

[2] An artifact is the tangible result of an activity or task performed during the lifecycle of a project.

**Appendix II**

## Major Contributors to This Report

Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Director
Jody Kitazono, Audit Manager
Bret Hunter, Lead Auditor
Larry Reimer, Senior Auditor
Chanda Stratton, Senior Auditor

## Appendix III

# Report Distribution List

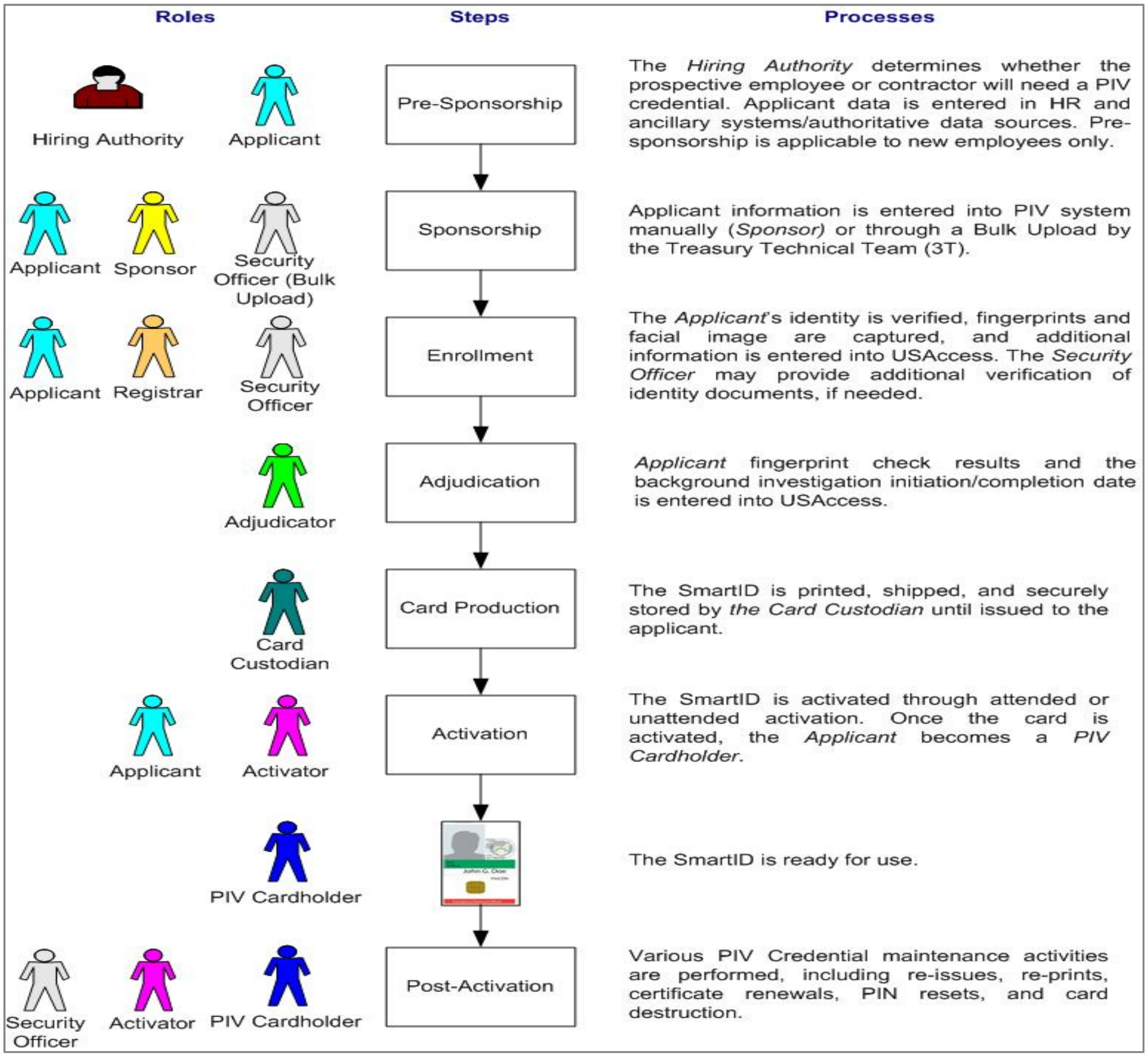
Commissioner  C
Office of the Commissioner – Attn:  Chief of Staff  C
Deputy Commissioner for Operations Support  OS
Deputy Commissioner for Services and Enforcement  SE
Associate Chief Information Officer, Cybersecurity  OS:CTO:C
Chief Counsel  CC
National Taxpayer Advocate  TA
Director, Office of Legislative Affairs  CL:LA
Director, Office of Program Evaluation and Risk Analysis  RAS:O
Office of Internal Control  OS:CFO:CPIC:IC
Audit Liaison:  Cybersecurity  OS:CTO:C

## Appendix IV

# Internal Revenue Service Personal Identity Verification Card Issuance and Use Graphics

This appendix presents the IRS PIV card program, which involves multiple steps, data sources, and personnel. Figure 1 depicts the basic IRS PIV card (also called SmartID) issuance process.

### Figure 1: IRS PIV Card Issuance Process



The *Hiring Authority* determines whether the prospective employee or contractor will need a PIV credential. Applicant data is entered in HR and ancillary systems/authoritative data sources. Pre-sponsorship is applicable to new employees only.

Applicant information is entered into PIV system manually (*Sponsor)* or through a Bulk Upload by the Treasury Technical Team (3T).

The *Applicant*'s identity is verified, fingerprints and facial image are captured, and additional information is entered into USAccess. The *Security Officer* may provide additional verification of identity documents, if needed.

*Applicant* fingerprint check results and the background investigation initiation/completion date is entered into USAccess.

The SmartID is printed, shipped, and securely stored by *the Card Custodian* until issued to the applicant.

The SmartID is activated through attended or unattended activation. Once the card is activated, the *Applicant* becomes a *PIV Cardholder*.

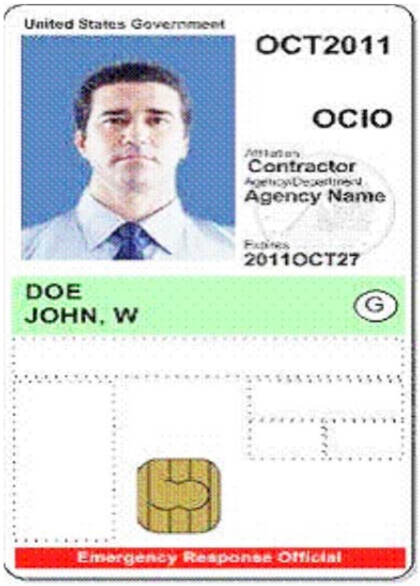
The SmartID is ready for use.

Various PIV Credential maintenance activities are performed, including re-issues, re-prints, certificate renewals, PIN resets, and card destruction.

*Source: IRS HSPD-12 Project Management Office policies and processes.*

The PIV card itself is coded with digital information which identifies an employee using various attributes. The digital information is read by card readers at entrances to, or within, IRS facilities to gain physical access to those facilities, or by computers to gain logical access to computers, networks, or applications. The card also includes visible identifiers for human verification such as a photo, name, title, and agency. Figure 2 provides an example of a typical PIV card.

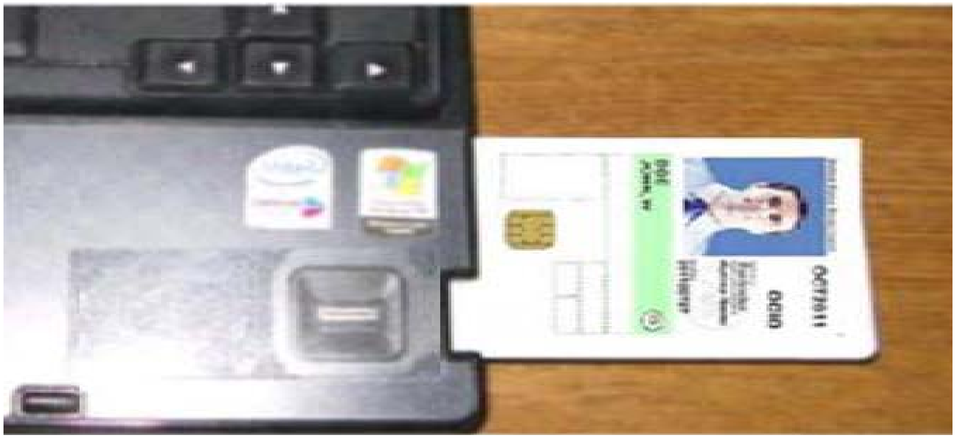
**Figure 2: Typical PIV Card**



*Source: IRS Mandatory SmartID User Guide.*

Once access is gained to an IRS facility, the PIV card is inserted into an IRS computer. Figure 3 provides an example of how a PIV card is inserted into a card reader within a computer.

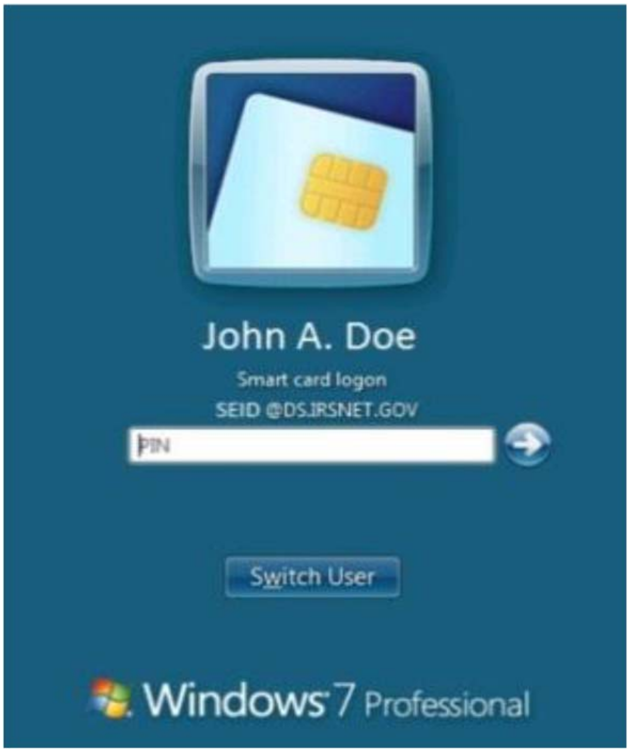
**Figure 3: Example of How to Insert a PIV Card**



*Source: IRS Mandatory SmartID User Guide.*

Once the PIV card is inserted into the computer, software reads the information on the PIV card and asks the user to enter his or her PIN.  Figure 4 illustrates the screen asking for the user's PIN.

**Figure 4:  Screen Asking for User's PIN**

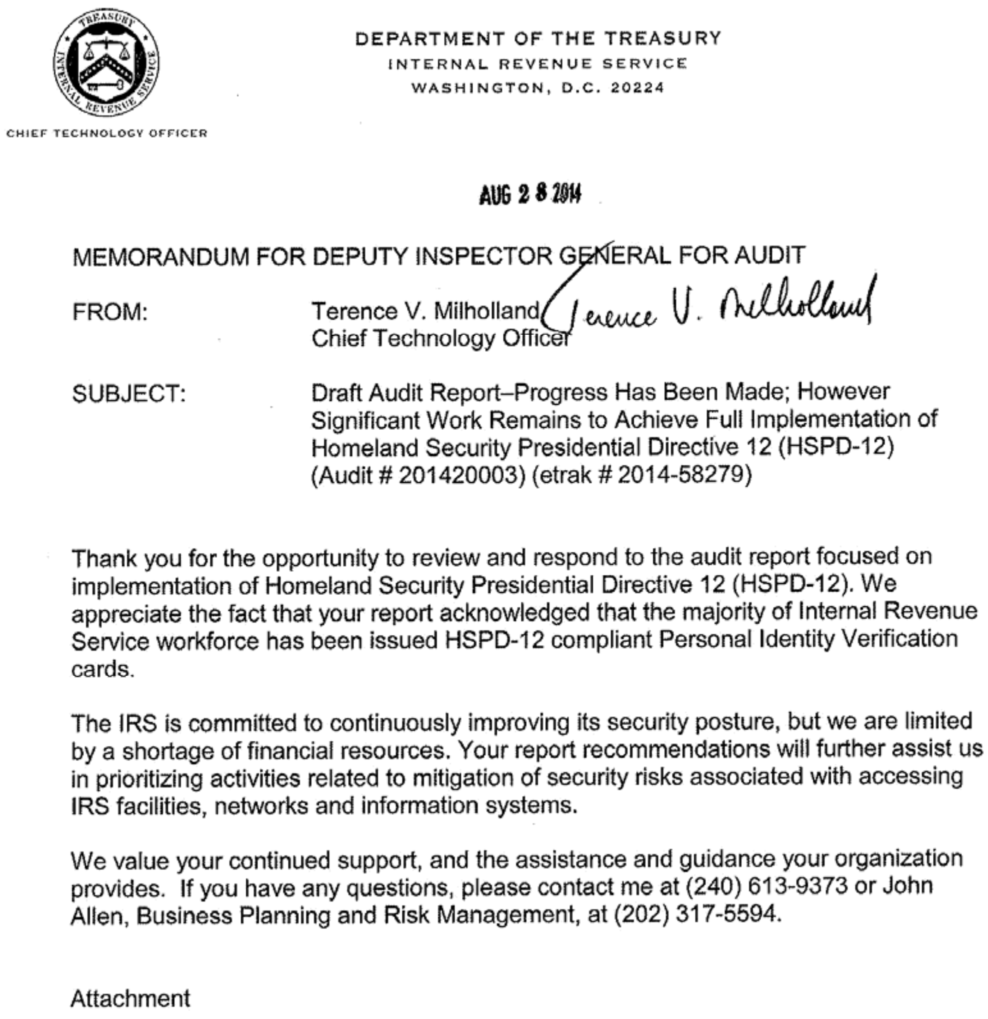


*Source:  IRS Mandatory SmartID User Guide.*

After the employee enters his or her PIN, the employee has access to the IRS computer and network.

## Appendix V

# *Management's Response to the Draft Report*



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

CHIEF TECHNOLOGY OFFICER

AUG 2 8 2014

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

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

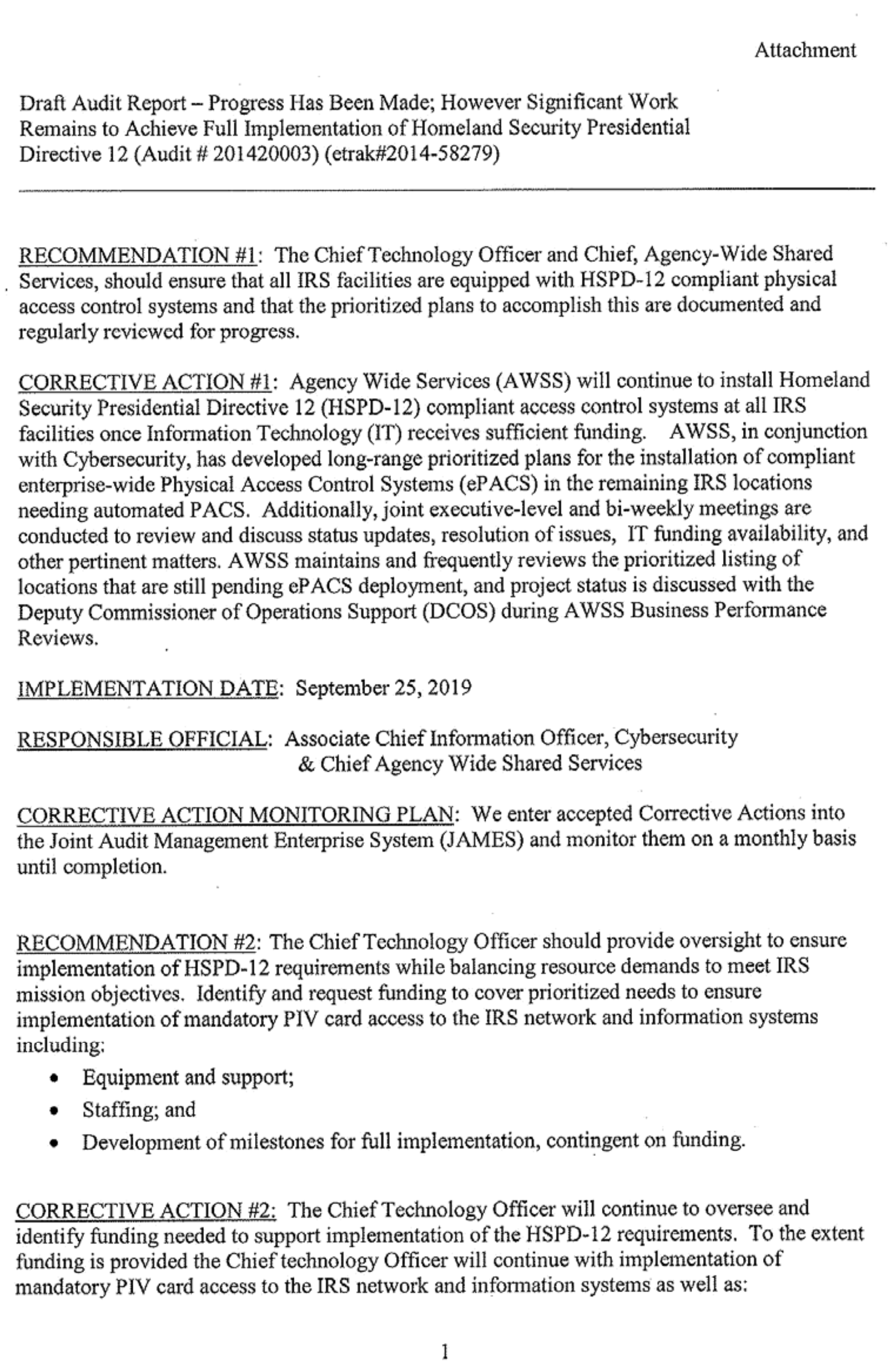
SUBJECT: Draft Audit Report–Progress Has Been Made; However Significant Work Remains to Achieve Full Implementation of Homeland Security Presidential Directive 12 (HSPD-12) (Audit # 201420003) (etrak # 2014-58279)

Thank you for the opportunity to review and respond to the audit report focused on implementation of Homeland Security Presidential Directive 12 (HSPD-12). We appreciate the fact that your report acknowledged that the majority of Internal Revenue Service workforce has been issued HSPD-12 compliant Personal Identity Verification cards.

The IRS is committed to continuously improving its security posture, but we are limited by a shortage of financial resources. Your report recommendations will further assist us in prioritizing activities related to mitigation of security risks associated with accessing IRS facilities, networks and information systems.

We value your continued support, and the assistance and guidance your organization provides. If you have any questions, please contact me at (240) 613-9373 or John Allen, Business Planning and Risk Management, at (202) 317-5594.

Attachment



Attachment

Draft Audit Report – Progress Has Been Made; However Significant Work Remains to Achieve Full Implementation of Homeland Security Presidential Directive 12 (Audit # 201420003) (etrak#2014-58279)

---

RECOMMENDATION #1: The Chief Technology Officer and Chief, Agency-Wide Shared Services, should ensure that all IRS facilities are equipped with HSPD-12 compliant physical access control systems and that the prioritized plans to accomplish this are documented and regularly reviewed for progress.

CORRECTIVE ACTION #1: Agency Wide Services (AWSS) will continue to install Homeland Security Presidential Directive 12 (HSPD-12) compliant access control systems at all IRS facilities once Information Technology (IT) receives sufficient funding. AWSS, in conjunction with Cybersecurity, has developed long-range prioritized plans for the installation of compliant enterprise-wide Physical Access Control Systems (ePACS) in the remaining IRS locations needing automated PACS. Additionally, joint executive-level and bi-weekly meetings are conducted to review and discuss status updates, resolution of issues, IT funding availability, and other pertinent matters. AWSS maintains and frequently reviews the prioritized listing of locations that are still pending ePACS deployment, and project status is discussed with the Deputy Commissioner of Operations Support (DCOS) during AWSS Business Performance Reviews.

IMPLEMENTATION DATE: September 25, 2019

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity
& Chief Agency Wide Shared Services

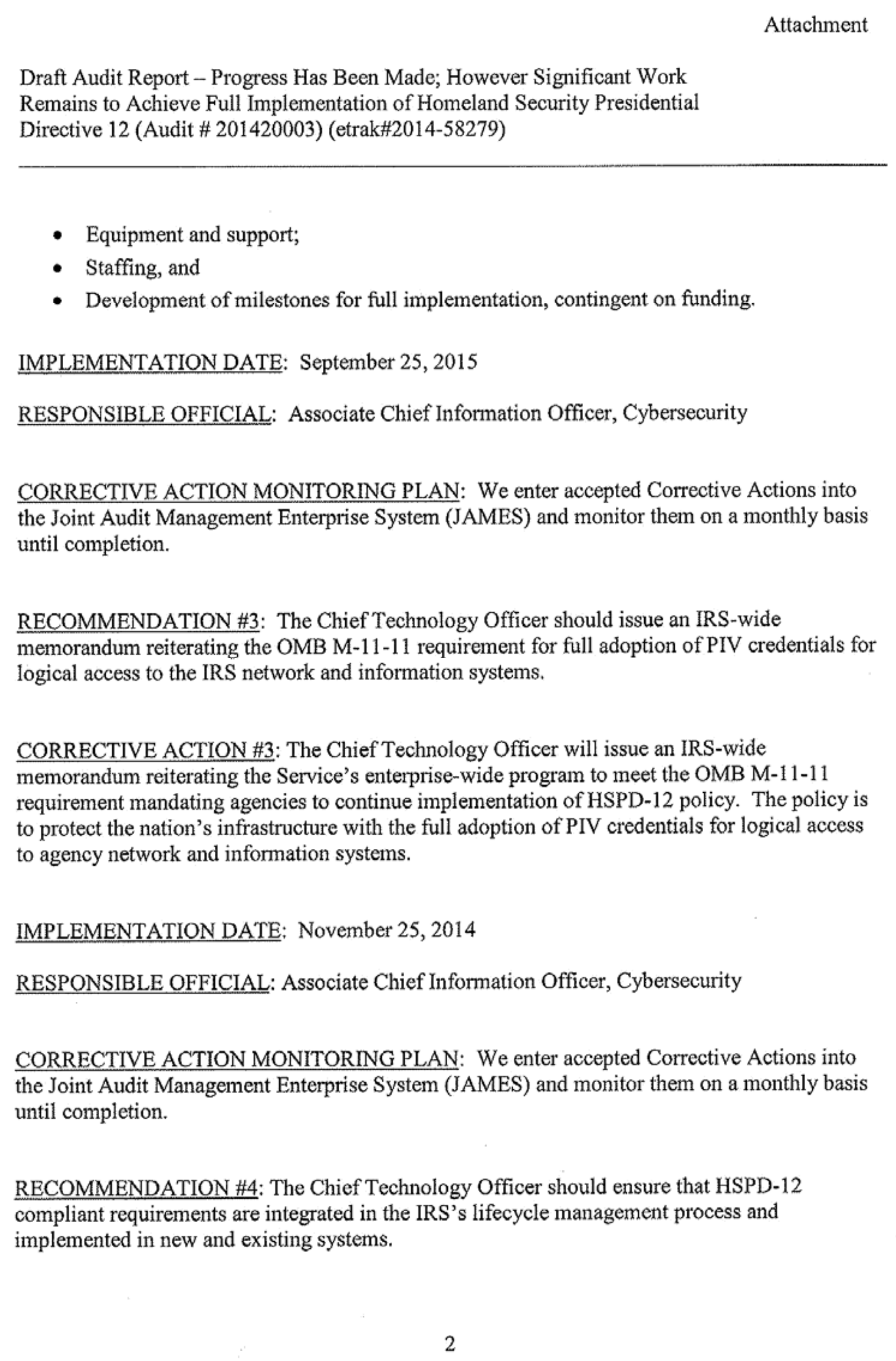
CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #2: The Chief Technology Officer should provide oversight to ensure implementation of HSPD-12 requirements while balancing resource demands to meet IRS mission objectives. Identify and request funding to cover prioritized needs to ensure implementation of mandatory PIV card access to the IRS network and information systems including:

- Equipment and support;
- Staffing; and
- Development of milestones for full implementation, contingent on funding.

CORRECTIVE ACTION #2: The Chief Technology Officer will continue to oversee and identify funding needed to support implementation of the HSPD-12 requirements. To the extent funding is provided the Chief technology Officer will continue with implementation of mandatory PIV card access to the IRS network and information systems as well as:

1



- Equipment and support;
- Staffing, and
- Development of milestones for full implementation, contingent on funding.

IMPLEMENTATION DATE: September 25, 2015

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

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

RECOMMENDATION #3: The Chief Technology Officer should issue an IRS-wide memorandum reiterating the OMB M-11-11 requirement for full adoption of PIV credentials for logical access to the IRS network and information systems.

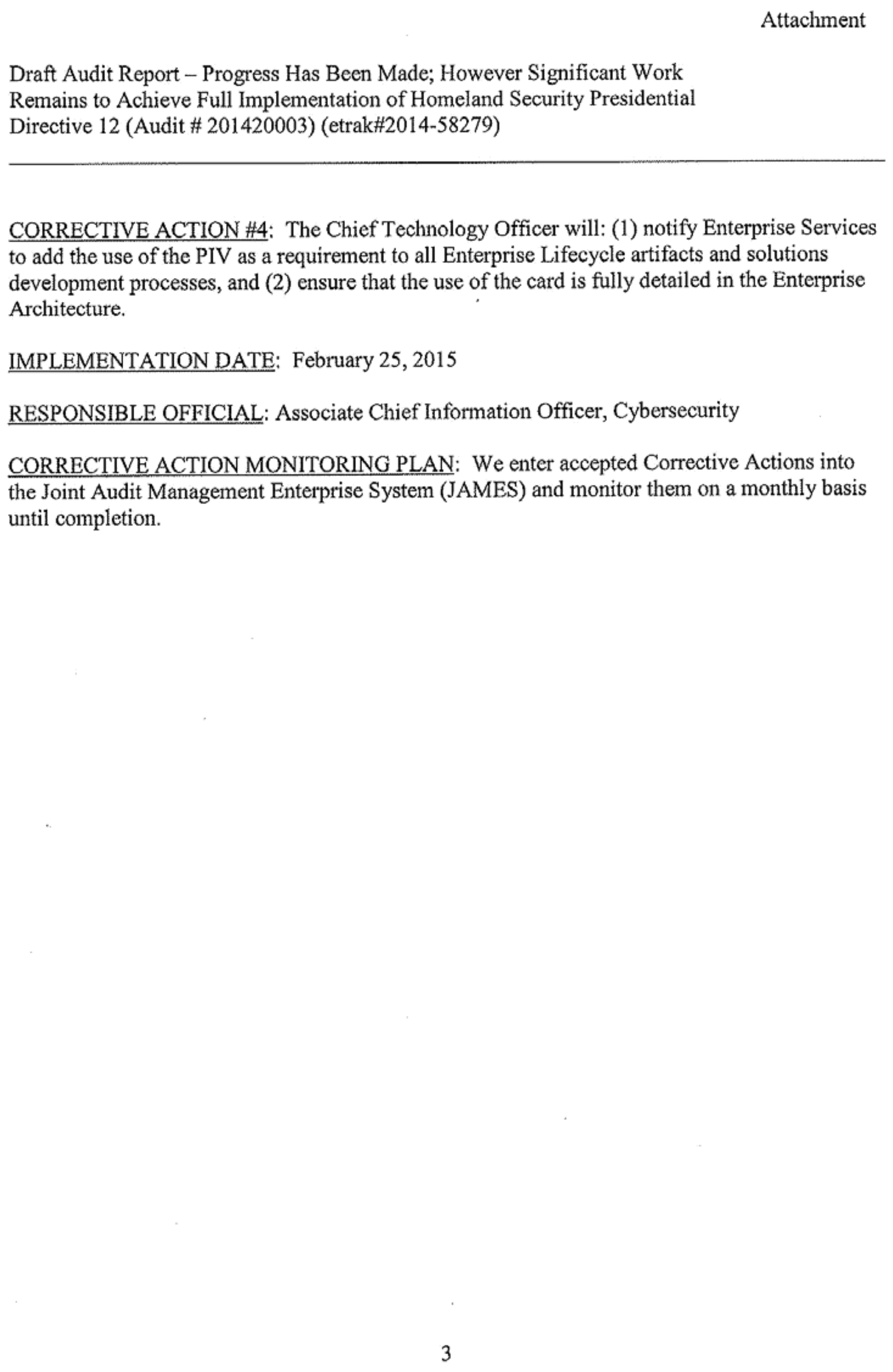
CORRECTIVE ACTION #3: The Chief Technology Officer will issue an IRS-wide memorandum reiterating the Service's enterprise-wide program to meet the OMB M-11-11 requirement mandating agencies to continue implementation of HSPD-12 policy. The policy is to protect the nation's infrastructure with the full adoption of PIV credentials for logical access to agency network and information systems.

IMPLEMENTATION DATE: November 25, 2014

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

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

RECOMMENDATION #4: The Chief Technology Officer should ensure that HSPD-12 compliant requirements are integrated in the IRS's lifecycle management process and implemented in new and existing systems.



Attachment

Draft Audit Report – Progress Has Been Made; However Significant Work Remains to Achieve Full Implementation of Homeland Security Presidential Directive 12 (Audit # 201420003) (etrak#2014-58279)

CORRECTIVE ACTION #4: The Chief Technology Officer will: (1) notify Enterprise Services to add the use of the PIV as a requirement to all Enterprise Lifecycle artifacts and solutions development processes, and (2) ensure that the use of the card is fully detailed in the Enterprise Architecture.

IMPLEMENTATION DATE: February 25, 2015

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

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