U.S. Securities and Exchange Commission

Office of Inspector General

Office of Audits

The SEC's Implementation of and Compliance with Homeland Security Presidential Directive 12

March 31, 2011
Report No. 481

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

OFFICE OF
INSPECTOR GENERAL

MEMORANDUM

March 31, 2011

To: Diego T. Ruiz, Executive Director, Office of the Executive Director
Jeffrey A. Risinger, Associate Executive Director, Office of Human Resources
Sharon Sheehan, Associate Executive Director, Office of Administrative Services
Thomas A. Bayer, Director, Office of Information Technology

From: H. David Kotz, Inspector General, Office of Inspector General (OIG)

Subject: *The SEC's Implementation of and Compliance with HSPD-12,* Report No. 481

This memorandum transmits the U.S. Securities and Exchange Commission OIG's final report detailing the results on our audit of the SEC's implementation of and compliance with HSPD-12. This audit was conducted as part of our continuous effort to assess management of the Commission's programs and operations and as a part of our annual audit plan.

The final report contains 25 recommendations which if fully implemented should ensure the Commission's full compliance with the HSPD-12 directive. The respective offices concurred with all the report's recommendations. Your written response to the draft report is included in Appendix VI.

Within the next 45 days, please provide the OIG with a written corrective action plan that is designed to address the report's recommendations. The corrective action plan should include information such as the responsible official/point of contact, timeframes for completing required actions, and milestones identifying how you will address the recommendations.

Should you have any questions regarding this report, please do not hesitate to contact me. We appreciate the courtesy and cooperation that you and your staff extended to our auditor during this audit.

Attachment

cc: Kayla J. Gillan, Deputy Chief of Staff, Office of the Chairman
Luis A. Aguilar, Commissioner
Troy A. Paredes, Commissioner
Elisse B. Walter, Commissioner
Jeffery Heslop, Chief Operating Officer, Office of the Chief Operations Officer
Cristin Fair, Acting Deputy Director, Office of Human Resources
Beth Blackwood, Assistant Director, Office of Administrative Services, Office of Security and Business Operations
Lewis W. Walker, Deputy Director, Chief Technology Officer, Office of Information Technology

The SEC's Implementation of and Compliance with Homeland Security Presidential Directive 12

Executive Summary

Background. On August 27, 2004, President George W. Bush signed Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*. This directive requires federal agencies to have programs in place to ensure that identification issued by each agency to federal employees and contractors meets a common standard. Those standards and technical specifications were set forth in Federal Information Processing Standards Publication (FIPS) 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors,* which was initially issued by the Department of Commerce's National Institute of Standards and Technology (NIST) on February 25, 2005, and revised in March 2006. On August 5, 2005, the Office of Management and Budget (OMB) issued memorandum M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 -- Policy for a Common Identification Standard for Federal Employees and Contractors* (M-05-24), which provided implementation instructions for HSPD-12 and FIPS 201.

The U.S. Securities and Exchange Commission (SEC) has implemented a collaborative effort to comply with HSPD-12 among three SEC offices: the Office of Information Technology (OIT), the Office of Administrative Services (OAS), and the Office of Human Resources (OHR). OIT is responsible for overseeing the implementation of the HSPD-12 program, assigning roles and responsibilities as requested by OHR's Personnel Security Branch management, and for implementing technological solutions for the use of HSPD-12 for identification and authentication to SEC logical information systems. OAS is responsible for enrolling PIV credentials (also referred to as PIV cards or HSPD-12 badges)[1] into its physical access control system and providing temporary SEC-issued badges while employees or contractors are awaiting receipt of their PIV credentials. OHR is responsible for the most essential component of the SEC's implementation of and compliance with HSPD-12, which is sponsoring and adjudicating the background investigation of an applicant. Further, OHR is responsible for sponsoring the employee or contractor for a PIV credential, adjudicating the results of the background investigation (including fingerprints), granting reciprocity as applicable, and informing OIT and OAS that the employee

[1] A "PIV card" is defined as "[a] physical artifact (e.g., identity card, "smart" card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable)." FIPS 201-1, Appendix F, Page 73, http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf.

or contractor is eligible for access to SEC facilities and authorized technology systems.

OMB M-05-24 provided multiple milestones for departments and agencies to achieve in their implementation of HSPD-12. As of the date of this report, the SEC has not met all of the milestones outlined in M-05-24. The SEC has informed OMB, through its quarterly reporting, that it will complete the issuance of PIV credentials (i.e., HSPD-12 badges) to all employees and contractors by June 2011, integration of PIV credentials with logical access systems by December 2011, and integration of PIV credentials with physical access control systems by June 2011.

Objectives. The primary objective of the audit of the SEC's implementation of and compliance with HSPD-12 is to determine if the SEC is fully compliant with HSPD-12 and the implementing standards and guidance. The OIG's specific audit objectives were as follows:

- Evaluate whether the SEC has adequate controls and the necessary processes and procedures to perform background investigations, adjudicate results, and issue credentials.

- Evaluate the roles and responsibilities for the HSPD-12 initiative among the various SEC offices involved in the process, including OAS, OHR, and OIT.

- Assess compliance with HSPD-12 and determine whether all the necessary equipment has been purchased to implement HSPD-12 throughout the SEC.

- Evaluate whether the HSPD-12 processes and procedures are consistently applied throughout the SEC (i.e., at SEC headquarters and the regional offices).

Prior OIG Reports and Memoranda. Four prior OIG reports and memoranda are relevant to this audit:

- OIG Report of Investigation No. OIG-544, *OIT Contract Employees Given Access to SEC Buildings and Computer Systems for Several Weeks Before Background Investigation Clearance,* issued on January 20, 2011, which contained four recommendations to strengthen management controls pertaining to contractor access to SEC facilities and information systems.
- OIG Inspection Report No. 434, *Background Investigations,* issued on March 28, 2008, which contained nine recommendations to strengthen management controls over OHR's background investigation program.

- OIG Investigative Memorandum No. G-444, *Law Student Observer Program,* issued on June 29, 2006, which contained three recommendations to strengthen management controls over OHR's background investigation program, specifically for interns selected through the SEC's Law Student Observer Program.
- OIG Audit Memorandum No. 39, *Operations Center Building Security*, issued on July 14, 2005, which contained three recommendations to strengthen management controls over building security at the SEC Operations Center located in Alexandria, Virginia.

Results. The OIG audit found deficiencies in nearly every aspect of the SEC's HSPD-12 program, as well as significant concerns about the SEC's authority to determine eligibility for access to classified information and the current process for granting temporary access to SEC facilities.

We found that the SEC has missed virtually all the deadlines established by OMB guidance for implementation of HSPD-12. M-05-24 required agencies to develop a plan and begin the required background investigations for current employees who did not have an initiated or successfully adjudicated investigation on record by October 27, 2005.[2] Our audit found no formal documentation of any such plan and, we were thus unable to confirm if the SEC ever satisfied this requirement. M-05-24 further required agencies to verify and/or complete background investigations for all current employees, excluding those who have been employed by the federal government over 15 years, by October 27, 2007.[3] Our audit found that the SEC did not verify and/or complete background investigations for all current employees, excluding those who have been employed by the federal government more than 15 years, until March or April of 2009 -- approximately a year and a half after the October 27, 2007, completion date required by M-05-24. Further, M-05-24 required, "For individuals who have been federal department or agency employees over 15 years, a new investigation may be delayed, commensurate with risk, but must be completed no later than October 27, 2008."[4] Our audit found that as of December 31, 2010, the SEC has not verified and/or completed background investigations for 1,263 employees who have more than 15 years of federal government service.

M-05-24 also required agencies to develop a plan and begin the required background investigations for all current contractors who did not have a successfully adjudicated investigation on record by October 27, 2005.[5] Our audit found that the SEC has not developed a plan commensurate with risk, for completion of background investigations for all current contractors who do not have a successfully adjudicated investigation on record. We also found that the

[2] OMB Memorandum M-05-24, *Implementation for Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*, page 6. http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf.
[3] M-05-24, page 6, http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf.
[4] M-05-24, page 6, http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf.
[5] M-05-24, page 6, http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf.

SEC is currently unable to determine the actual number of contractors who are employed by the SEC; thus, there is a serious question as to whether the SEC accurately reported its statistics related to contractors in its December 31, 2010, quarterly HSPD-12 Implementation Status Report to OMB.

Further, M-05-24 required that agencies adopt and accredit a registration process and initiate an appropriate background investigation for all new employees and contractors by October 27, 2005.[6] We found that the SEC, as it reported to OMB, only began issuing PIV credentials to all new employees and contractors as part of the onboarding process in April 2010, and the SEC has failed to meet the October 27, 2005 deadline by several years.

During our audit, we compared the SEC's September 2010 quarterly HSPD-12 Implementation Status Report with reports of (1) other federal financial agencies and (2) federal agencies of similar size to the SEC. We found that the SEC lagged well behind both other agencies with similar missions and those with similar numbers of employees. As of September 30, 2010, the SEC reported that only 61 percent of its employees and contractors had been issued PIV cards, while all of the other agencies we reviewed reported that they had issued PIV cards to over 90 percent of their employees and contractors.

Our audit also found that since June 30, 2008, the SEC has adjudicated and determined the eligibility of 26 employees and contractors to access classified information without receipt of delegated authority from the Director of National Intelligence (DNI), which Executive Order 13467 established as the final authority to designate an agency to make such determinations. We also found that the SEC's determinations of eligibility for access to classified information were based on incorrect policies and procedures. Additionally, we found that OAS's Physical Security Branch is making eligibility determinations for applicants seeking temporary access to SEC facilities without the proper authority. Moreover, the Physical Security Branch is not using the appropriate standards for making these determinations.

Our audit also found that the SEC's regional offices have not consistently enrolled PIV badges into the SEC's physical access control system. In addition, the SEC's badging policy is outdated and does not include policies and procedures for issuing and revoking badges, or for requiring the use of the PIV credentials as the common means of authentication for access to SEC facilities and information systems. We further found that OHR's Personnel Security Branch does not have policies or procedures specific to adjudicating foreign nationals.

Further, our audit determined that OIT's asset inventory does not account for keyboards (some of which contain card readers that could be used to authenticate PIV credentials) and lacks detail necessary to identify laptops that

[6] M-05-24, page 6, http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf.

have card readers. Without this information, OIT might unnecessarily purchase new keyboards and laptops with card readers or external card readers. Our audit also disclosed that OIT employs two full-time registrars, who are responsible for validating an applicant's identity, ensuring the successful completion of background checks, and providing approval for the issuance of a PIV credential to the applicant. Our audit found that the SEC expended a total of approximately $144,000 to employ registrars between June 2009 and December 2010, which would have been avoided if the SEC had implemented HSPD-12 within the required timeframes. Moreover, our audit found that based on the average number of transactions processed per day, the SEC only requires one part-time registrar. We also found that the SEC did not conduct an analysis before employing a second full-time registrar or consider alternatives, such as splitting the time of the existing registrar between both facilities or hiring a part-time registrar to work at the Operations Center. As a result, the SEC has expended unnecessary costs to employ two full-time registrars when, based on an eight-hour workday, the registrars combined are spending an average of only two hours per day processing transactions. Our audit concluded that the SEC could save $108,000 annually by employing one part-time registrar, rather than two full-time registrars.

Finally, the audit found that OAS's Physical Security Branch is not maintaining visitor record logs in accordance with the National Archives and Records Administration's (NARA) General Records Schedule retention requirement of two years. Because the Physical Security Branch is retaining such records for only 90 days, it is unable to analyze visitor logs effectively to determine if visitors are accessing the agency inappropriately (i.e., circumventing the badging process if they require access for more than six months).

Summary of Recommendations. Our audit determined that numerous improvements were required in order to ensure that the SEC becomes compliant with HSPD-12. Specifically, we recommended that:

(1) OHR immediately prepare formal documented plans for initiating background investigations for all current employees who do not have successfully adjudicated background investigations on record, commensurate with risk;

(2) OHR immediately, but no later than 90 days after the issuance of this report, initiate background investigations for all current employees who do not have successfully adjudicated investigations on record, commensurate with risk;

(3) OAS should identify and develop a consolidated list of all contractors employed by the SEC, and coordinate with the Contracting Officer's Technical Representatives and

Inspection and Acceptance Officials to implement policies and procedures for ensuring that the list remains up to date;

(4) OAS provide the OHR's Personnel Security Branch with a copy of the up-to-date consolidated contractor list on a weekly basis;

(5) OHR's Personnel Security Branch, upon receipt of the up-to-date consolidated contractor list, should determine which contractors do not have successfully adjudicated investigations on record and develop a plan to begin the required background investigations immediately;

(6) OHR, upon receipt of the up-to-date consolidated contractor list, ensure that accurate status reporting has been made to OMB;

(7) OED discontinue adjudicating all eligibility determinations for access to classified information or holding a sensitive position until the SEC has received an appropriate delegation of authority to conduct such determinations from the DNI;

(8) OED identify all eligibility determinations for access to classified information or holding a sensitive position adjudicated by the SEC since June 30, 2008, and, upon receipt of authority from the DNI, conduct a quality control assessment to ensure that the determinations were conducted in accordance with the uniform policies and procedures developed by DNI;

(9) OED, upon receipt of authority from the DNI to make eligibility determinations for access to classified information or holding a sensitive position, should use the DNI's uniform policies and procedures developed by DNI when making such determinations;.

(10) OAS immediately discontinue making eligibility determinations for persons requiring temporary access to SEC facilities or information systems without proper authorization;

(11) OAS immediately provide OHR's Personnel Security Branch with a list of all persons who have been provided or denied access based on the Physical Security Branch's risk assessments, as well as a copy of all fingerprints records, supporting documentation, and the results of the risk assessments;

(12) OHR, in coordination with OAS, should develop policies and procedures for determining the eligibility of contractors, visitors, and guests requiring temporary access to SEC's facilities or information systems;

(13) OAS communicate to regional office staff its expectations for enrolling PIV credentials into their physical access control systems and using the PIV credential as the primary badge for physical access to SEC facilities;

(14) OAS require administrative officers in the regional offices, or designated points of contact, to enroll PIV cards in the SEC's physical access control system;

(15) OED communicate to all SEC employees and contractors their responsibility to inform the appropriate regional office official that they have been issued a Personal Identity Verification card so the card can be enrolled into the SEC's physical access control system;

(16) OED develop and implement a policy requiring the PIV badge to be used as a common and primary means of authentication for physical and logical access;

(17) OAS revise and update its *Identification Cards, Press Passes and Proximity Access Control Cards* policy to reflect current and proper practices for issuance and revocation of badges, including PIV cards, to SEC employees and contractors at all SEC facilities, post the revised policy on the SEC's intranet site, and communicate the new policy to all employees and contracting officials;

(18) OAS develop and implement a plan to systematically revoke all SEC-issued badges for all employees and contractors who have been issued HSPD-12 badges and ensure that the plan is implemented no later than six months after the date this report is issued;

(19) OHR develop, implement, and post in multiple locations (e.g., SEC intranet site, human resources offices, regional offices) and provide at contractor orientation its appeals procedures for individuals who are denied credentials or whose credentials are revoked;

(20) OHR develop internal policies and procedures for suitability determinations for foreign nationals;

(21) OIT immediately conduct an audit of its inventory to identify and track all keyboards and laptops that contain card readers;

(22) OIT promptly deploy appropriate technology (e.g., laptops with internal card readers, keyboards with card readers, or external card readers) to employees and contractors who do not have card readers;

(23) OIT eliminate one full-time registrar and split the time of the other full-time registrar between the Operations Center and headquarters locations;

(24) OAS retain visitor control logs for a period not less than two years after final entry or two years after date of document in accordance with the NARA's General Records Schedule; and

(25) OAS perform periodic analysis of visitor data to ensure that visitors are not circumventing the HSPD-12 requirements.

TABLE OF CONTENTS

Appendices

Tables

Background and Objectives

Background

Issuance of HSPD-12 and Implementing Standards and Guidance. On August 27, 2004, President George W. Bush signed Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*.[7] This directive requires federal agencies to have programs in place to ensure that the identifications issued by each agency to federal employees and contractors meet a common standard. Those standards and technical specifications were set forth in Federal Information Processing Standards Publication (FIPS) 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors,* which was initially issued by the National Institute of Standards and Technology (NIST) on February 25, 2005, and updated in March 2006 with the issuance of FIPS 201-1. On August 5, 2005, the Office of Management and Budget (OMB) issued memorandum M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors* (M-05-24), which provides instructions for implementing HSPD-12 and FIPS 201.[8] Further, M-05-24 required all employees and contractors needing access for periods longer than six months to comply with the background investigation requirements of FIPS 201. FIPS 201 requires the completion of a background investigation consisting of a National Agency Check with Inquiries (NACI) or other Office of Personnel Management (OPM) or National Security community investigation.[9]

Implementation Requirements. As described in M-05-24, department and agency implementation of HSPD-12 contains two parts: Part 1 – Common Identification, Security, and Privacy Requirements and Part 2 – Government-wide Uniformity and Interoperability. Part 1 defines the minimum requirements for a federal personal identification system that meets the control and security objectives of HSPD-12, including personal identify proofing, registration, and issuance process for employees and contractors. Part 2 details the specifications used to support the technical interoperability among departments and agencies, which include card elements, system interfaces, and security

[7] Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors* (http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html).
[8] Office of Management and Budget (OMB) Memorandum M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractor*, (M-05-24), August 5, 2005 (http://www.whitehouse.gov/omb/memoranda/fy2005/m05-24.pdf).
[9] A NACI is the "basic and minimum investigation required on all new federal employees consisting of a NAC [National Agency Check] with written inquiries and searches of records covering specific areas of an individual's background during the past five years (inquiries sent to current and past employers, schools attended, references, and local law enforcement authorities)." Federal Information Processing Standards Publication 201-1 (FIPS 201-1), *Personal Identity Verification (PIV) of Federal Employees and Contractors*, March 2006, Appendix C, page 66, http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf.

controls required to securely store and retrieve data from the card. M-05-24 provides dates by which all departments and agencies should complete their implementation of HSPD-12, as reflected in Table 1 below:

Table 1: Dates and Actions That Should Be Completed by Each Department and Agency

Date	Agency Action
06/27/2005	Submit implementation plans to OMB
10/27/2005	Comply with FIPS 201, Part I
10/27/2006	Begin compliance with FIPS 201, Part 2
10/27/2007	Verify and/or complete background investigations for all current employees and contractors
10/27/2008	Complete background investigations for all federal departments or agency employees employed over 15 years

Source: OMB Memorandum M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*, August 5, 2005, page 4, Section 2.B.

Further, agencies are required to acquire and use federally approved products and services that are compliant with FIPS 201 and included on the approved products list. In addition, departments and agencies are encouraged to use the acquisition services provided by the General Services Administration (GSA). For small departments and agencies where it may not be cost-effective to procure their own products or services, M-05-24 indicates that GSA will identify agency sponsors to provide the services. The U.S. Securities and Exchange Commission (SEC or Commission) determined that it would be cost-prohibitive to acquire and use its own federally approved products and services. As a result, in August 2008, the SEC entered into an interagency agreement with GSA to provide these products and services.

Furthermore, under FIPS 201, agencies are required to report annually on the numbers of agency-issued credentials, including (1) general credentials and (2) special-risk credentials. The SEC reports this data to OMB and posts its HSPD-12 Implementation Status Report on the SEC's website quarterly.

Roles and Responsibilities. The SEC implemented a collaborative effort to comply with HSPD-12 among three SEC offices: the Office of Information Technology (OIT), the Office of Administrative Services (OAS), and the Office of Human Resources (OHR). OIT is responsible for overseeing the implementation of the HSPD-12 program, assigning roles and responsibilities as requested by OHR's Personnel Security Branch management, and implementing logical and technology solutions for the use of HSPD-12 for identification and authentication to SEC logical information systems. OAS is responsible for enrolling PIV credentials[10] into its physical access control system and providing temporary

[10] A "PIV card" is defined as "[a] physical artifact (e.g., identity card, "smart" card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and

SEC-issued badges while employees or contractors are awaiting receipt of their PIV credentials (also referred to as a PIV card or HSPD-12 badge).

OHR is responsible for the most essential component of the SEC's implementation of and compliance with HSPD-12, which is sponsoring and adjudicating the background investigation of an applicant. Further, OHR is responsible for sponsoring the employee or contractor for a PIV credential, adjudicating the results of the background investigation (including fingerprints), granting reciprocity as applicable, and informing OIT and OAS that the employee or contractor is eligible for access to the SEC facilities and authorized technology systems.

In addition to the three SEC offices, GSA, the Federal Bureau of Investigation (FBI), OPM, and the Director of National Intelligence (DNI) also have roles and responsibilities in the SEC's implementation of and compliance with HSPD-12. GSA is responsible for registering, issuing, and activating the PIV credentials on behalf of the SEC. The FBI is responsible for receiving fingerprints and providing results of the criminal record checks of employees or contractors to the SEC to be adjudicated prior to issuing SEC badges[11] or PIV credentials. OPM is responsible for providing oversight of, and developing and implementing uniform and consistent policies and procedures for, the completion of investigations and adjudications relating to suitability determinations and eligibility for logical and physical access. In addition, OPM designates agencies to adjudicate suitability eligibility determinations for logical and physical access. The DNI is responsible for the oversight of investigations and determination of eligibility for access to classified information, including developing uniform policies and procedures related to determinations of eligibility for access to classified information. Further, the DNI is responsible for delegating agencies the authority to determine eligibility to accessed classified information in accordance with Executive Order 12968, *Access to Classified Information*.

This collaborative effort requires diligence among all the SEC offices involved in the process, with a special emphasis on OHR, which is responsible for sponsoring the employee or contractor for the PIV credential and adjudicating the results of the background investigation. Below is a description of the responsibilities of each role that is held by OHR staff members.

- **Sponsor:** As of December 13, 2010, the SEC had three sponsors.[12] A sponsor's role is to substantiate the need for a PIV credential to be issued

verifiable)." FIPS 201-1, Appendix F, Page 73, http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf.

[11] SEC-issued badges include several types of badges: an SEC government employee badge that has a dark blue background; an SEC contractor employee badge that has an orange background; an on-site business badge that has a light blue background; an intern badge that has a red background; a badge issued to employees of other federal agencies who are working at the SEC pursuant to interagency agreements that has a black bar with stripes; a visitor badge; and an employee day pass that is paper.

[12] This information was obtained from the GSA USAccess program, *Role Assignment Report*, printed 12/13/2010 at 4:35:06 pm.

to an applicant. The sponsor is responsible for entering the applicant's biographical information and other data into the GSA USAccess system once a request has been received from a contracting official or OHR's Talent Management Branches. The sponsors are located in the Personnel Security Branch within OHR.

- **Adjudicator:** As of December 13, 2010, the SEC had three adjudicators.[13] An adjudicator is responsible for recording the adjudication results of the applicant. A "positive" or "favorable" adjudication will initiate the PIV credential issuance process. Adjudicators are assigned within the Personnel Security Branch.

In addition, the roles and responsibilities of the GSA Managed Service Office (MSO)[14] staff includes registering, issuing, and activating PIV credentials, which are significant functions in the implementation of and compliance with HSPD-12. MSO staff roles are described below.

- **Registrar:** The registrar is responsible for validating the applicant's identity (i.e., identity proofing) by inspecting two identity documents, one of which must be a government-issued photo identification. Also, the registrar collects biographical information from the identity documents, takes a photograph, and collects rolled fingerprints from the applicant. Registers are not specific to an agency, but rather are provided by the MSO. Registrars are located in MSO offices throughout the United States. The SEC has two registrars located on site, one at headquarters and another at the Operations Center.

- **Issuer:** The issuance process is completely automated and, as a consequence, a physical person is not required to complete the task of issuing the PIV credential. USAccess, the GSA application used by MSO to process the PIV credential request, produces the PIV credential and issues the PIV card to the MSO for activation.[15]

- **Activator:** The activator is responsible for verifying that the applicant is the person to whom the PIV card should be issued and assists the applicant in activating the PIV credential.[16]

Implementation Delays. In the early stages of implementing HSPD-12, as referenced in the OIG Inspection *Background Investigations,* Report No. 434,

[13] This information was obtained from the GSA USAccess program, *Role Assignment Report*, printed 12/13/2010 at 4:35:06 pm.
[14] A GSA MSO is a managed shared service solution that simplifies the process of procuring and maintaining PIV-compliant credentials and provides turn-key services to federal agencies in satisfying the requirements of OMB Memorandum M-05-24. For additional information, see http://www.fedidcard.gov/aboutmso.aspx.
[15] PIV Card Issuer Operations Plan, GSA MSO, CM# GSA-DI-0000129-1.4.0, p. 35.
[16] PIV Card Issuer Operations Plan, GSA MSO, CM# GSA-DI-0000129-1.4.0, p. 37.

issued on March 28, 2008, the SEC faced multiple challenges, such as a lack of resources to adjudicate the number of applicants and a paper-based onboarding process. However, since 2008, Personnel Security has increased its staff from one adjudicator to three adjudicators and has automated the onboarding process.

Implementation Status. The SEC has provided to OPM, on a quarterly basis, HSPD-12 Implementation Status Reports.[17] As of December 2010, the SEC informed OMB that it would continue to not comply with several deadlines required by M-05-24, including (1) completion of the issuance of PIV credentials to all employees and contractors, (2) adjudications or verifications of background investigations for all employees and contractors, (3) integration of PIV credentials with logical access systems, and (4) integration of PIV credentials with physical access systems. In addition, the SEC informed OMB in its December 2010 quarterly report that 1,238[18] of its approximately 3,907 employees[19] and 785[20] of its approximately 1,427 contractors[21] still require PIV credentials. Further, the SEC informed OMB that it would complete the integration of PIV credentials with its logical access systems by December 2011.

Objectives

In accordance with its annual audit plan, the OIG conducted an audit of the Commission's implementation of HSPD-12. The primary objective of this audit of the SEC's implementation of and compliance with HSPD-12 is to determine if the SEC is fully compliant with HSPD-12 and the implementing standards and guidance. The specific audit objectives were as follows:

- Evaluate whether the SEC has adequate controls and the necessary processes and procedures to perform background investigations, adjudicate results, and issue credentials.

- Evaluate the roles and responsibilities for the HSPD-12 initiative among

[17] The most recent Implementation Status Report, issued in December 2010, can be found at http://www.sec.gov/about/piv_report_for_omb.pdf.
[18] This number represents the "Number of Employees requiring PIV credentials" as reported by the SEC to OMB in December 2010 in its HSPD-12 Implementation Status Report, http://www.sec.gov/about/piv_report_for_omb.pdf (accessed on 02/01/2011).
[19] This number represents the sum of the "Total Number of PIV credentials Issued to Employees" (2,669) and "Number of Employees requiring PIV credentials" (1,238) as reported by the SEC to OMB in December 2010 in its HSPD-12 Implementation Status Report, http://www.sec.gov/about/piv_report_for_omb.pdf (accessed on 02/01/2011).
[20] This number represents the "Number of Contractors requiring PIV credentials" as reported by the SEC to OMB on December 2010 in its HSPD-12 Implementation Status Report, http://www.sec.gov/about/piv_report_for_omb.pdf (accessed on 02/01/2011).
[21] The total number of contractors was calculated using data provided in the SEC's December 2010 quarterly HSPD-12 Implementation Status Report. The total number of contractors (1,427) is the sum of the "Number of Contractors requiring PIV credentials" (785) and "Total Number of PIV Credentials Issued to Contractors" (642), although Personnel Security Branch staff acknowledged that they were unsure of the actual total number of SEC contractors.

the various offices involved in the process, including OAS, OHR, and OIT.

- Assess compliance with HSPD-12 and determine whether all the necessary equipment has been purchased to implement HSPD-12 throughout the SEC.

- Evaluate whether the HSPD-12 processes and procedures are consistently applied throughout the SEC (i.e., at headquarters and the regional offices).

Findings and Recommendations

Finding 1: The SEC Has Not Issued PIV Credentials to All Employees and Contractors and Lags Behind Other Federal Agencies in Implementing HSPD-12

> The SEC has not issued PIV credentials to all employees and contractors in accordance with HSPD-12. In addition, the SEC does not have a formal, documented plan for completing the implementation of HSPD-12 and is unable to account for all of the contractors employed by the agency. As a result, the SEC is not compliant with HSPD-12 and lags behind other federal financial agencies and agencies of similar size in implementing the directive.

On August 27, 2004, the President signed HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, which requires the development and agency implementation of a mandatory, government-wide standard for secure and reliable forms of identification for federal employees and contractors. The OMB, on August 5, 2005, issued Implementation Standards, OMB Memorandum, M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors (*M-05-24), which provides guidance for agencies' implementation of HSPD-12. M-05-24 provides specific requirements and deadlines for departments and agencies to achieve for issuing the PIV credentials (also referred to as HSPD-12 badges or cards) to employees and contractors. Under HSPD-12, department and agency heads conduct background investigations, adjudicate the results, and issue identity credentials to their employees and contractors who require long-term access (i.e., more than six months) to federally controlled facilities and/or information systems.[22] M-05-24 also specifically provides instructions for developing plans, completing background investigations, and issuing credentials to current employees, current contractors, new employees, and new contractors.

Current SEC Employees

M-05-24 requires agencies to develop a plan and begin the required background investigations for current employees who did not have an initiated or successfully adjudicated investigation (i.e., a NACI or other OPM or National Security community investigation) on record by October 27, 2005. In addition, M-05-24

[22] M-05-24, p. 2, http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf.

requires agencies to verify and/or complete background investigations for all current employees, excluding those who have been employed by the federal government over 15 years, by October 27, 2007.[23] Further, M-05-24 Implementation Standard stated, "For individuals who have been federal department or agency employees over 15 years, a new investigation may be delayed, commensurate with risk, but must be completed no later than October 27, 2008."[24]

Plan and Initiation of Background Investigations for Current Employees. During interviews with Personnel Security Branch staff, we were informed that the Personnel Security Branch has developed an informal plan to conduct background investigations, adjudicate results, and issue credentials for employees with less than 15 years of federal service, based on the number of staff in each division or office. However, we found no formal documentation of this plan and thus were unable to confirm if the SEC ever satisfied the requirement that a plan be developed by October 27, 2005. We note that in a previous inspection conducted by the OIG in March 2008 with respect to its audit on *Background Investigations*,[25] we similarly found that "the Office of Human Resources [did] not have a formal plan of how it intend[ed] to meet this requirement [to develop a plan by October 27, 2005]. Additionally, due to limited resources, OHR ha[d] not focused its efforts on meeting this requirement." Consistent with our finding in the OIG's March 2008 *Background Investigations* report, we found in this audit that background investigations were not begun for all current employees who did not have an initiated or completed investigation on record by the October 27, 2005 deadline, due to the lack of resources. Although we were unable to confirm an exact date for when the required background investigations were actually initiated, the Personnel Security Branch informed us that background investigations were completed for all current employees with less than 15 years of federal service in or about March or April of 2009.

Verification and/or Completion of Background Investigations for All Current Employees With Less Than 15 Years Federal Service. As described above, OIG found that the SEC did not verify and/or complete background investigations for all current employees, excluding those who have been employed by the federal government more than 15 years, until March or April of 2009 — approximately a year and a half after the October 27, 2007, completion date required by M-05-24.[26] We were informed by the Personnel Security Branch that the SEC did not meet this deadline due to a lack of resources.

[23] M-05-24, page 6, http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf
[24] M-05-24, page 6, http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf
[25] *Background Investigations*, Inspection Report No. 434, March 28, 2008. http://www.sec-oig.gov/Reports/AuditsInspections/2008/434final.pdf.
[26] We were unable to confirm the exact date of completion. The Personnel Security Branch informed us that the SEC verified and/or completed background investigations for all current employees, excluding those who have been employed by the federal government over 15 years, around the March/April 2009 timeframe.

Investigations for Employees With More Than 15 Years of Federal Service. As of December 31, 2010, the SEC had not verified and/or completed background investigations for 1,263[27] employees who have more than 15 years of federal government service. As a result, the SEC did not meet the October 27, 2008, deadline requirement set forth in M-05-24. Moreover, based on interviews with Personnel Security Branch staff, we learned that the SEC has not developed a formal, documented plan, commensurate with risk, to complete these background investigations. Although the Personnel Security Branch represented to us that the Branch has an informal plan, this informal plan (based upon the size of divisions or offices) is not consistent with M-05-24, which requires that outstanding background investigations be conducted commensurate with risk. By not conducting the outstanding background investigations commensurate with risk, the agency has allowed employees to continue to occupy key agency positions without having a successfully adjudicated background investigation equivalent to or greater than a NACI. For example, based on the SEC Executive Director's (ED) Notice of Personnel Action dated January 3, 2010, the ED's position is classified as critical sensitive risk. However, the ED does not have a successfully adjudicated background investigation completed that is equivalent to or greater than a NACI, which is the minimum background investigation level required. During the course of this audit, on or about December 14, 2010, a background investigation was initiated for the ED; however, the background investigation has not yet been completed.

During an interview with the ED, we were informed that all remaining background investigations would be initiated in January 2011, and adjudications and the verification of background investigations for employees requiring investigations would be completed by March 31, 2011. In the SEC's December 2010 quarterly HSPD-12 the Implementation Status Report to OMB, the SEC indicated that it would complete adjudication and verification of background investigations for all employees and contractors by March 2011. However, we were informed on February 2, 2011, that the SEC had still not begun the background investigations for 1,263 employees who have been employed by the federal government for over 15 years. The ED indicated that the delay in processing these investigations is due to workload demands. As previously mentioned, this is the same justification provided for the prior delay in implementing HSPD-12 with respect to employees with less than 15 years of federal service. The initiation, verification, and completion of background investigations for all current employees with less than 15 years of federal service occurred during a period when the Personnel Security Branch employed only one adjudicator for background investigations for the entire agency. In 2008, the Personnel Security Branch increased the number of adjudicators from one to three. Further, the federal government has been operating under a continuing resolution and hiring has therefore been restricted; as a result, we believe that the Personnel Security

[27] This number represents the total number of employees with more than 15 years of federal service who either (1) had a background investigation completed more than 15 years ago that was at least equivalent to a NACI; or (2) never had a background investigation that was at least equivalent to a NACI completed.

Branch has had adequate time to initiate and adjudicate background investigations for all employees who still require investigations.

Moreover, the continuous delays related to the Personnel Security Branch's not initiating background investigations for current employees with more than 15 years of federal service may likely result in further delays in the SEC's implementation of HSPD-12. As a consequence, the SEC may have to report to OMB in its March 31, 2011, quarterly HSPD-12 Implementation Status Report yet another new completion date.

Current SEC Contractors

M-05-24 required agencies to develop a plan and begin the required background investigations for all current contractors who did not have a successfully adjudicated investigation on record by October 27, 2005.[28] In addition, M-05-24 provided that the requirement should be phased in to coincide with the contract renewal cycle, but no later than October 27, 2007.[29] In the SEC's quarterly HSPD-12 Implementation status report provided to OMB on December 31, 2010, the SEC reported that 785[30] of approximately 1,427 contractors[31] required PIV credentials.

Based on interviews with Personnel Security Branch staff, we understand that the SEC has begun initiating required background investigations and adjudicating those investigations for current contractors for whom they have received a request from the contractor's assigned Contracting Officer's Technical Representative (COTR) and the Inspection and Acceptance Officials (IOA). However, a formal documented plan has not been prepared for ensuring that background investigations are completed for all contractors employed by the SEC. While the Personnel Security Branch receives a consolidated, up-to-date list of current SEC employees from the SEC's payroll system, it has not received a consolidated, up-to-date list of all contractors who are employed by the SEC who require long-term access to SEC-controlled facilities or SEC information systems. Consequently, we found that the Personnel Security Branch is unable to accurately determine which contractors have a successfully adjudicated background investigation on record, unless it has been processed at the request of the COTR.

[28] M-05-24, p. 6, http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf.
[29] M-05-24, p. 6, http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf.
[30] This number represented the ""Number of Contractors requiring PIV credentials" as reported by the SEC to OMB on December 2010 in its HSPD 12 Implementation Status Report, http://www.sec.gov/about/piv_report_for_omb.pdf.
[31] The total number of contractors was calculated using data provided in the SEC's December 31, 2010, quarterly HSPD-12 Implementation Status Report. The total number of contractors (1,427) is the sum of the "Number of Contractors requiring PIV credentials" (785) and "Total Number of PIV Credentials Issued to Contractors" (642); however, Personnel Security Branch staff acknowledge that they were unsure of the actual total number of SEC contractors.

We contacted the OAS Office of Acquisitions (OA) to obtain an up-to-date list of all current contractors. The contractor list OA provided was incomplete and outdated. Through interviews with OA staff, we learned that OA has attempted to maintain a complete list of contractor personnel, but has not been successful due to lack of coordination between OA and COTRs regarding when a contractor is still employed at the SEC or has been separated.[32] Consequently, the Personnel Security Branch has been unable to determine the total number of contractors who require background investigations that meet the minimum requirements of HSPD-12.

As a result of not being able to determine the actual number of contractors who are employed by the SEC, we were unable to verify whether the SEC has accurately reported to OMB its HSPD-12 implementation status as it relates to contractors. In fact, the Personnel Security Branch indicated that in the SEC's most recent submission to OMB, the information provided was only to the best of the Personnel Security Branch's knowledge because the office does not know with certainty how many contractors have departed the SEC at any given time. Therefore, it is possible that the SEC may have inaccurately reported its statistics related to contractors in its December 31, 2010, quarterly HSPD-12 Implementation Status Report. Further, without an accurate and complete record of all contractors employed by the SEC, the Commission may be unable to meet the HSPD-12 implementation status dates that it provided to OMB on December 31, 2010, to complete the adjudications and verification of background investigations for all contractors by March 2011 and issuance of PIV credentials to all contractors by June 2011.

Further, we found that the SEC has not developed a plan, commensurate with risk, or begun required background investigations for all current contractors who do not have a successfully adjudicated investigation on record.

New SEC Employees and Contractors

M-05-24 requires that agencies adopt and accredit a registration process and initiate a NACI or equivalent investigation for all new employees and contractors by October 27, 2005.[33] As reported to OMB, the SEC only began issuing PIV credentials to all new employees and contractors as part of the onboarding process in April 2010 and has failed to meet the NACI October 27, 2005, deadline. According to the Personnel Security Branch, the SEC did not meet this deadline due to lack of resources.

We were informed that the Personnel Security Branch has hired two additional adjudicators since 2008, which increased the number of adjudicators to three. In addition, as noted above, we found that as of April 2010, the SEC had adopted a

[32] We have been informed that in the future, the list of current contractors will not be maintained by OA but instead by the OAS Physical Security Branch.
[33] M-05-24, p. 5, http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf.

registration process for all identity credentials issued to new SEC employees and contractors who require long-term access to SEC-controlled facilities or information systems. In addition, we found that the SEC has initiated a process for conducting a NACI or equivalent investigation prior to credential issuance.

Benchmarking

We compared the SEC's December 2010 quarterly HSPD-12 Implementation Status Report with reports of (1) other federal financial agencies and (2) agencies of similar size. We determined that the SEC lags behind other agencies with similar missions (i.e., financial regulators) and/or with approximately the same number of employees and contractors with completed NACIs. We examined the HSPD-12 implementation status of four financial agencies, including the SEC. These agencies were selected because they did not have any errors in their reporting, OMB indicated that their data quality was considered "acceptable," and the date of their status report was equivalent to the date of SEC's status report. The financial agencies selected for our comparison were the Farm Credit Administration, the Department of the Treasury, and the Board of Governors of the Federal Reserve System (Federal Reserve Board). See Table 2 below.

Table 2: Comparison of SEC to Other Federal Financial Agencies

Name of Agency	Date of Status Report Used	Percentage of Employees and Contractors with Completed NACIs	Percentage of Employees and Contractors with Issued PIV Cards
Securities and Exchange Commission	09/30/2010	82%	61%
Farm Credit Administration	09/30/2010	99%	95%
Department of the Treasury	09/30/2010	99%	90%
Federal Reserve Board	09/30/2010	95%	92%

Source: Generated by OIG.

In addition, the OIG examined two additional federal agencies that are similar in size to the SEC (based on the total number of employees requiring PIV credentials reported to OMB) by reviewing their HSPD-12 Implementation Status Reports submitted to OMB as of September 30, 2010. The agencies selected were the Department of Education and the Nuclear Regulatory Commission. See Table 3 below.

Table 3: Comparison of SEC to Other Similarly Sized Federal Departments or Agencies

Name of Agency	Date of Status Report Used	Number of Employees and Contractors to Receive PIV Cards (Q4, FY 2010)	Percentage of Employees and Contractors with Completed NACIs	Percentage of Employees and Contractors with Issued PIV Cards
Securities and Exchange Commission	09/30/2010	4,971	82%	61%
Department of Education	09/30/2010	4,243	99%	99%
Nuclear Regulatory Commission	09/30/2010	5,567	100%	100%

Source: Generated by OIG.

As Tables 2 and 3 illustrate, as of September 30, 2010, the SEC reported that only 61 percent of its employees and contractors had been issued PIV cards, while its counterparts reported that they had issued PIV cards to over 90 percent of their employees and contractors. Also, as Tables 2 and 3 show, not only has the SEC failed to meet the requirements of HSPD-12, but it also lags well behind other federal financial agencies and similarly sized federal agencies or departments in implementing HSPD-12, specifically as it relates to the percentage of employees and contractors who have been issued PIV cards.

Summary

The SEC did not comply with the HSPD-12 requirements and deadlines for current employees and contractors or for new employees and contractors. Specifically, we found that SEC did not achieve any of the agency action deadlines specified in M-05-24. In particular, we found that the SEC did not develop a formal plan or verify and complete background investigations for all current employees with less than 15 years of federal service prior to the October 27, 2007, deadline. Additionally, we found that the SEC has not completed background investigations for all employees who have more than 15 years of federal service and thus did not meet the October 27, 2008, deadline. We also found that the informal plan developed by the Personnel Security Branch to implement HSPD-12 is not commensurate with risk, but rather was developed based on the population of divisions and offices with employees requiring background investigations.

We further determined that the SEC does not have a complete, up-to-date list of all contractors who are employed by the SEC. Furthermore, we were unable to verify that the SEC is accurately reporting its HSPD-12 implementation status to OMB as it pertains to contractors due to the lack of a complete and consolidated list of contractors. Also, we found that the SEC has not developed a plan or

adjudicated background investigations for all current contractors. In addition, we found that the SEC significantly delayed issuing PIV credentials as required to new employees and contractors, due to a claimed lack of resources.

As a result of the continuous delays resulting from Personnel Security Branch's not initiating new background investigations for current employees who have been employed by the federal government for more than 15 years, it is likely that the SEC will have to further delay its implementation of HSPD-12 and will have to report a new estimated completion date to OMB in its March 31, 2011, quarterly HSPD-12 Implementation Status Report. In addition, by not developing and issuing an adequate implementation plan for the completion of background investigations for current employees and contractors who still require background investigations, as required by M-05-24, the SEC may not be able to meet the March 2011 date for completion of adjudications and verification of background investigations for all current contractors and employees or issue PIV credentials to all contractors and employees by June 2011.

Further, due to the lack of tracking of contractors' employment status, the SEC cannot ensure that the PIV credential statistics reported to OMB related to contractors are reliable and accurate. In addition, the SEC is not realizing the full benefits of the PIV credentials due to the lack of full implementation. By not fully implementing PIV credentials for physical and logical access, the SEC is unable to realize the significant benefits of the PIV credentials, such as greater security by virtue of enhanced authentication, increased government efficiency because all federal employees have the same identification cards, reduced identity fraud because the cards are assigned a personal identification number (PIN) for each employee associated with the card, and protection of personal privacy resulting from encryption of the personal data contained in the cards.

Recommendation 1:

The Office of Human Resources should immediately prepare formal, documented plans for initiating background investigations for all current employees who do not have successfully adjudicated background investigations on record, commensurate with risk.

Management Comments. OHR concurred with this recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased that OHR concurred with this recommendation.

Recommendation 2:

The Office of Human Resources should immediately, but no later than 90 days after the issuance of this report, initiate background investigations for all current employees who do not have successfully adjudicated investigations on record, commensurate with risk.

Management Comments. OHR concurred with this recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased that OHR concurred with this recommendation.

Recommendation 3:

The Office of Administrative Services should identify and develop a consolidated list of all contractors who are employed by the Commission. In addition, the Office of Administrative Services should coordinate with the Contracting Officer's Technical Representatives and Inspection and Acceptance Officials to implement policies and procedures for ensuring that the list remains up to date.

Management Comments. OAS concurred with this recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased that OAS concurred with this recommendation.

Recommendation 4:

The Office of Administrative Services should provide the Office of Human Resources Personnel Security Branch with a copy of the up-to-date consolidated contractor list on a weekly basis.

Management Comments. OAS concurred with the recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased that OAS concurred with this recommendation.

Recommendation 5:

Upon receipt of the up-to-date consolidated contractor list, the Office of Human Resources Personnel Security Branch should determine which contractors do not have successfully adjudicated background investigations on record and develop a plan to begin the required background investigations immediately.

Management Comments. OHR concurred with the recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased that OHR concurred with this recommendation.

Recommendation 6:

Upon receipt of the up-to-date consolidated contractor list, the Office of Human Resources should ensure that accurate status reporting has been made to the Office of Management and Budget.

Management Comments. OHR concurred with the recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased that OHR concurred with this recommendation.

Finding 2: The SEC Does Not Have the Authority to Determine Eligibility of a Person for Access to Classified Information

> Since June 30, 2008, the SEC has adjudicated and determined the eligibility of 26 employees and contractors to access classified information without receipt of delegated authority from the Director of National Intelligence (DNI). We found that these determinations were based on incorrect policies and procedures and as a result found that the determinations for access to classified information that were made by the Office of Executive Director (OED) may not meet the minimum requirements of the adjudicative guidelines set forth by DNI.

On January 27, 1986, the SEC Chairman's Office transferred authority over the personnel security function to the OED and designated the ED as the Commission's Personnel Security Officer and the Director of Personnel (i.e., the Associate Executive Director for Human Resources) as the Assistant Personnel Security Officer. The transfer of this authority made the ED responsible for the overall management of the SEC's background investigation program and OHR responsible for administering the program on behalf of the agency. Since this delegation, the OED has retained responsibility for adjudicating the background investigations of employees and contractors who require access to classified information and assigned OHR's Personnel Security Branch responsibility for conducting suitability determinations for employees, contractors, and persons requiring temporary access.

On June 30, 2008, President George W. Bush signed Executive Order 13467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*,[34] which designated the DNI as "the Security Executive Agent." According to Executive Order 13467, the DNI, among other things, is "responsible for developing uniform and consistent policies and procedures to ensure the effective, efficient, and timely completion of investigations and adjudications relating to determinations of eligibility for access to classified information or eligibility to hold a sensitive position"; serves as the final authority to designate an agency to determine eligibility for access to classified information in accordance with Executive Order 12968 of August 4, 1995;[35] and ensures

[34] Executive Order 13467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information,* June 30, 2008, http://www.fas.org/irp/offdocs/eo/eo-13467.htm.

[35] Executive Order 12968, *Access to Classified Information*, August 4, 1995, http://www.fas.org/sgp/clinton/eo12968.html. Executive Order 12968 order establishes a uniform federal personnel security program for employees who will be considered for initial or continued access to classified information.

reciprocal recognition of eligibility for access to classified information among the agencies.

Consistent with Executive Order 13467, on October 1, 2008, the DNI issued Intelligence Community Directive (ICD) Number 704, *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and other Controlled Access Program Information*.[36] This directive, among other things, requires the application of uniform personnel security standards and procedures to facilitate effective initial vetting, continuing personnel security evaluation, and reciprocity throughout the intelligence community.

We contacted the DNI on January 5, 2011, to determine if the DNI had provided the SEC with the designated authority to determine eligibility for access to classified information. A Chief Assessment Officer at the DNI stated that based on a review of DNI records, the SEC had not received authority to make eligibility determinations for access to classified information.

We found that although the SEC has received authority from OPM to make suitability determinations,[37] the SEC has not received the authority from the DNI to make eligibility determinations for access to classified information or the holding of a sensitive position. We found that notwithstanding this lack of authority, the SEC has made eligibility determinations for access to classified information and submitted to OPM adjudication actions for 26 employees and contractors for access to classified information. In addition, we found that the OED is using materials[38] obtained from training sessions that OED personnel have attended to make eligibility determinations for access to classified information or the holding of sensitive positions, rather than the policies and procedures issued by the DNI, which include ICD 704.[39] As a result, the OED may have made determinations that particular employees or contractors should receive access to classified information when, in fact, had the OED used the

[36] Intelligence Community Directive, Number 704, *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information*, effective October 1, 2008, http://www.fas.org/irp/dni/icd/icd-704.pdf.

[37] See 5 C.F.R. § 731.103 – Delegation to agencies,http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=eff878f50f31e1d9d9fe7f90c34674ee&rgn=div5&view=text&node=5:2.0.1.1.7&idno=5, which states, "(a) Subject to the limitations and requirements of paragraphs (f) and (g) of this section, OPM delegates to the heads of agencies authority for making suitability determinations and taking suitability actions (including limited, agency-specific debarments under §731.205) in cases involving *applicants* for and *appointees* to covered positions in the agency."

[38] The training materials used by OED personnel to make eligibility determinations to access classified information were *Revised Adjudicative Guidelines for Determining Eligibility for Access to Classified Information*, issued by the White House, on December 29, 2005; in a memorandum for William Leonard, Director of Information Security Oversight Office, Subject: Adjudicative Guidelines, Signed by Stephen J. Hadley, Assistant to the President for National Security Affairs; and *Investigative Standards for Background Investigations for Access to Classified Information*, updated December 2004.

[39] While we found that there were similarities between the training materials used by the OED for making eligibility determinations to access classified information and the appropriate eligibility standards outlined in DNI's ICD 704, there were also several differences and certain requirements in ICD 704 that were not in the training materials utilized by the OED.

uniform policies and procedures developed by the DNI, these determinations may have not been favorable, based on the DNI's guidelines. Additionally, if any of the 26 employees or contractors were to transfer to another federal department or agency, they could potentially be granted reciprocity when, in fact, they might not have properly received a favorable determination.

We contacted the SEC Chairman's Correspondence Office[40] to determine if the SEC had received notice of Executive Order 13467 from the White House and if, upon receipt, the Chairman's Correspondence Office provided the OED with a copy of the Executive Order and required the OED to take action to implement it. The Chairman's Correspondence Office indicated that it did not have a record of receiving a copy of Executive Order 13467 (which the Correspondence Office indicated was unusual), but that if it had received the Executive Order, it would have referred the Executive Order to the OED for action. We were informed by OED staff that they were aware of the issuance of Executive Order 13467; however, they were unaware of any actions that were required on their part.

In summary, we determined that the SEC has acted outside of its authority in making determinations of eligibility for access to classified information. Further, we found that the 26 determinations of eligibility for access to classified information made between June 2008 and December 2010 were not based on the uniform policies and procedures developed by the DNI. Further, we found that the determinations of eligibility for access to classified information that were made by the OED might receive improper reciprocal recognition by other agencies, which could result in persons receiving access to classified information when, in fact, they should not have been granted eligibility to receive such access.

Recommendation 7:

The Office of Executive Director should discontinue adjudicating all eligibility determinations for access to classified information or holding a sensitive position until the Securities and Exchange Commission has received an appropriate delegation of authority to conduct such determinations from the Director of National Intelligence.

Management Comments. OED concurred with the recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased that OED concurred with this recommendation.

[40] We contacted the Chairman's Correspondence Office on February 17, 2011, and February 23, 2011.

Recommendation 8:

The Office of Executive Director should identify all eligibility determinations for access to classified information or holding a sensitive position adjudicated by the Securities and Exchange Commission since June 30, 2008 and, upon receipt of authority from the Director of National Intelligence, conduct a quality control assessment to ensure that the determinations were conducted in accordance with the uniform policies and procedures developed by the Director of National Intelligence.

Management Comments. OED concurred with the recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased OED concurred with this recommendation.

Recommendation 9:

The Office of Executive Director, upon receipt of authority from the Director of National Intelligence to make eligibility determinations for access to classified information or holding a sensitive position, should use the uniform policies and procedures developed by the Director of National Intelligence when making such determinations.

Management Comments. OED concurred with the recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased OED concurred with this recommendation.

Finding 3: OAS's Physical Security Branch Is Making Eligibility Determinations for Applicants Seeking Temporary Access to SEC Facilities Without the Proper Authority

OAS's Physical Security Branch is making eligibility determinations for applicants seeking temporary access[41] to SEC facilities without the proper authority. Additionally, the Physical Security Branch is not using the appropriate standards for making these determinations. As a result,

[41] Temporary access is defined as access to SEC facilities or logical access to SEC information systems for a period of more than one day but less than six months.

applicants may unjustly be denied access to SEC facilities without the right to appeal.

According to 5 C.F.R. § 731.103, "OPM delegates to the heads of agencies authority for making suitability determinations and taking suitability actions . . . ."[42] As noted above, on January 27, 1986, the Chairman's Office transferred authority for the personnel security function to the OED and designated the ED as the Commission's Personnel Security Officer and the Director of Personnel (i.e., the Associate Executive Director for Human Resources) as the Assistant Personnel Security Officer. The transfer of this authority made the ED responsible for the overall management of the SEC's background investigation program and OHR's Personnel Security Branch responsible for administering the program on behalf of the agency. Similarly, the OHR intranet site states, "The Office of the Executive Director (OED) is responsible for overall management of the SEC's background investigation program, and OHR is responsible for administering the program."[43]

Executive Order 13467 defines "adjudication" as "the evaluation of pertinent data in a background investigation, as well as any other available information that is relevant and reliable, to determine whether a covered individual is: (i) suitable for Government employment; (ii) eligible for logical and physical access; (iii) eligible for access to classified information; (iv) eligible to hold a sensitive position; or (v) fit to perform work for or on behalf of the Government as a contractor employee."[44]

In the *Federal Managers' Financial Integrity Act Assurance Statement* submitted by OAS to the SEC Chairman on September 15, 2010, OAS stated, "We installed electronic fingerprinting equipment to enhance the process of performing criminal and background checks on employees, contractors, and intermittent vendors who need access to SEC facilities."[45]

During this audit, we found that the Physical Security Branch staff conduct risk assessments of contractors who require unescorted temporary access (i.e., for periods of less than six months) to SEC facilities based on fingerprint results that are received from the FBI, using an electronic fingerprint verification system called the Civilian Applicant System (CAS). We also learned that the Physical Security Branch staff use the CAS to collect fingerprints from temporary contractors who are seeking unescorted access (e.g., construction staff) and these fingerprints are then sent through the CAS system to the FBI. Within 24

[42] 5 CFR § 731.103, Delegation to agencies.
[43] http://insider.sec.gov/human_resources/hiring_staffing/background-security-clearances.html.
[44] Executive Order 13467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information,* June 30, 2008, http://www.fas.org/irp/offdocs/eo/eo-13467.htm.
[45] Memorandum to SEC Chairman Mary Schapiro from Sharon Sheehan, Associate Executive Director, Office of Administrative Services, Subject: *Federal Managers' Financial Integrity Act Assurance Statement*; September 15, 2010, p. 6.

hours, the FBI provides the Physical Security Branch with fingerprint results indicating if the applicant has a criminal record and, if so, the types of crimes the applicant has committed. Once the results are received in the CAS system, the Physical Security Branch staff review the results and conduct a risk assessment to determine whether the temporary contractor is an acceptable risk and can work within the SEC's facilities. If a favorable risk determination is made by Physical Security Branch personnel, an on-site business badge is issued to the temporary contractor. However, we found that the Physical Security Branch does not have formal, documented procedures for its risk assessment process or for the criteria it uses to determine the suitability of applicants.

Although we were informed in an interview that the Physical Security Branch does not "perform OHR adjudications," the Physical Security Branch acknowledged that it conducts "a risk assessment of the candidates to determine if the candidate poses a risk to the SEC staff or facilities." In interviews, the Physical Security Branch staff represented the following: "We (Physical Security Branch) determine whether or not the person is a risk to other SEC employees." Moreover, it is clear from the results of our audit that the Physical Security Branch is evaluating pertinent, relevant, and reliable data received from the FBI to determine whether a covered individual is fit to perform work for or on behalf of the government as a contractor employee. In conducting such evaluations, the Physical Security Branch is relying upon results from the FBI to determine if the person is of "acceptable risk" to perform work for or on behalf of the government. Thus, the Physical Security Branch is engaged in evaluating an individual's background data to determine eligibility for physical access to agency facilities and, therefore, is essentially performing an adjudication as that term is defined in Executive Order 13467.

The Physical Security Branch has no written policies and procedures for conducting its risk assessments and is not adhering to the OHR guidelines[46] for adjudications, which require uniformity in suitability case processes and adjudication. In addition, these guidelines assist in adjudicating cases using sound judgment, objectivity, and careful analysis, while ensuring that the procedures used and the results of the determination are consistent and not arbitrary.

Moreover, we were informed by the Physical Security Branch that the fingerprint and risk assessment results are not communicated to the Personnel Security Branch, even though the Personnel Security Branch is responsible for making suitability determinations and for maintaining the repository of records that are used in determining the eligibility of employees or contractors to access SEC facilities. We confirmed during interviews with Personnel Security Branch staff that the results of the Physical Security Branch's risk assessments are not provided to the Personnel Security Branch.

[46] OHR uses the Office of Personnel Management, Federal Investigative Services Division, *Suitability Processing Handbook*, September 2008, as guidelines for its suitability/background investigations program.

Accordingly, we found that the Physical Security Branch has been determining the eligibility of individuals for temporary access to SEC facilities without the authority to do and has not followed the appropriate standards in making these determinations. Consequently, the Physical Security Branch may have provided applicants access to SEC facilities where such access would have been denied had the case been adjudicated under the OHR guidelines. Alternatively, the Physical Security Branch may have unjustly denied persons access to SEC facilities, and those individuals would not have any right of appeal.

Recommendation 10:

The Office of Administrative Services should immediately discontinue making eligibility determinations without proper authorization for persons requiring temporary access to Securities and Exchange Commission facilities or information systems.

Management Comments. OAS concurred with the recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased OAS concurred with this recommendation.

Recommendation 11:

The Office of Administrative Service should immediately provide the Office of Human Resources Personnel Security Branch with a list of all persons who have been provided or denied access based on the Physical Security Branch's risk assessments, as well as a copy of all fingerprint records, supporting documentation, and the results of the risk assessments.

Management Comments. OAS concurred with the recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased that OAS concurred with this recommendation.

Recommendation 12:

The Office of Human Resources, in coordination with the Office of Administrative Services, should develop policies and procedures for determining the eligibility of contractors and visitors and guests requiring temporary access to Securities and Exchange Commission facilities or information systems.

Management Comments. OHR concurred with the recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased that OHR concurred with this recommendation.

Finding 4: PIV Cards Are Not Consistently Enrolled in the SEC's Physical Access Control System and Badge Requirements for Physical Access to SEC Facilities Have Not Been Communicated to All Employees and Contractors

The SEC's regional offices have not consistently enrolled PIV badges into the SEC's physical access control system. In addition, OAS has not communicated badging requirements for physical access to employees and contractors. As a result, the SEC has not met HSPD-12's requirement to use PIV cards for gaining physical access to SEC-controlled facilities and information systems.

HSPD-12 states, "As promptly as possible, but in no case later than eight months after the date of promulgation of the Standard, the heads of executive departments and agencies shall, to the maximum extent practicable, require the use of identification by federal employees and contractors that meets the Standard in gaining physical access to federally controlled facilities and logical access to federally controlled information systems."[47]

Additionally, NIST, Special Publication 800-116, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS),* states, "HSPD-12 mandates the establishment of a government-wide standard for identity credentials to improve physical security in federally controlled facilities."[48] It further notes, "HSPD-12 explicitly requires the use of PIV Cards 'in gaining physical access to federally controlled facilities and logical access to federally controlled information systems."[49]

Employees and contractors working at the SEC's headquarters and the Operations Center receive their PIV badges from a GSA registrar who is located in the SEC's badging office at headquarters. At the time an employee or contractor receives his or her badge from the GSA registrar, the employee or contractor is enrolled into the SEC's physical access control system, known as

[47] HSPD-12, http://csrc.nist.gov/drivers/documents/Presidential-Directive-Hspd-12.html.
[48] National Institute of Standards and Technology (NIST), Special Publication 800-116, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*, November 2008, p. 4 [footnote omitted], http://csrc.nist.gov/publications/nistpubs/800-116/SP800-116.pdf.
[49] NIST Special Publication 800-116, page 4, http://csrc.nist.gov/publications/nistpubs/800-116/SP800-116.pdf.

the Diebold Hirsh system. However, in the regional offices, employees and contractors receive their PIV badges (also referred to as credentials and HSPD-12 badges) at a GSA Managed Service Office (MSO), which is normally located off site. After receiving their PIV badges, these employees and contractors must return to their assigned regional office and inform their administrative officer (or other designated person) that they are in possession of the PIV badge in order for it to be enrolled into the SEC's physical access control system and/or a building-owned, proprietary physical access control system.

As part of our fieldwork, we conducted a survey of the SECs 11 regional offices[50] to determine if employees and contractors who have been issued HSPD-12 badges have had them enrolled into the SEC's physical access control system. All 11 regional offices responded to the survey and indicated that a physical access control system, either the Diebold Hirsh system or a building-owned proprietary system, is used to access the SEC's office space at the regional offices. However, based on the survey, as answered by the administrative officers in the regional offices, only 37 percent of the regional offices responded that employee badges are enrolled into the physical access system and only 46 percent responded that contractor badges are enrolled into the physical access control system. In fact, only 2 of the 11 regional offices that responded on this issue indicated that they have been notified by an SEC employee when an HSPD-12 badge has been issued to the employee, and only 1 of the 11 regional offices indicated that it either received an e-mail or phone call from the Personnel Security Branch notifying it of the issuance of an HSPD-12 badge. The remaining 7 regional offices responding on this issue stated that they are not notified when an employee has been issued an HSPD-12 badge.

OAS has informed us that it was unaware of any official guidance issued to agency staff or the regional offices requiring enrollment of PIV credentials into the SEC's physical access control system and further stated that the PIV credentials would be the primary physical access badge used by SEC employees and contractors. In addition, the Physical Security Branch advised us that enrollment of the PIV badge and SEC badges into the physical access control system is done locally at the regional offices and that the regional offices' administrative officers, not headquarters, are responsible for enrolling the HSPD-12 badges into the physical access control system. However, the OIG survey found that the administrative officers at the regional offices are not requiring the enrollment of PIV credentials into the SEC's physical access control system.

Additionally, we found that on October 2, 2006, OAS distributed a newsletter to Division/Office Heads; Regional Directors/District Administrators, administrative officers, and Budget Analysts that provided information regarding HSPD-12 and changes to the SEC's physical access control system that would take place to support the new PIV cards. However, the newsletter did not indicate that OAS

[50] The SEC's 11 regional offices include are Atlanta, Boston, Chicago, Denver, Fort Worth, Los Angeles, Miami, New York, Philadelphia, Salt Lake City, and San Francisco.

expected that the PIV credential would be the primary badge used by SEC employees and contractors.

We found that OAS's lack of guidance or communication of its expectations to regional offices' administrative officers (or other designated staff) regarding the enrollment of PIV badges in the SEC's physical access control system located within their specific regional office has resulted in the failure of administrative officers to understand management's expectations for enrolling PIV badges into the physical access control system. In addition, we found that administrative officers, or designated persons in charge of enrolling badges into the physical access control system, are not informed in most cases by OHR or the badge holders (i.e., SEC employees and contractors) that they are in possession of a PIV credential so it can be enrolled. As a result, the SEC has not met the HSPD-12's requirements to use the PIV cards to gain physical access to the SEC's regional office facilities and thus, has not taken advantage of the significant benefits of the PIV cards, as noted above, including greater security by virtue of enhanced authentication, increased government efficiency, reduction of identity fraud, and increased protection of personal privacy.

Recommendation 13:

The Office of Administrative Services should communicate to regional office staff its expectations for enrolling Personal Identity Verification credentials into their physical access control systems and using the Personal Identity Verification credential as the primary badge for physical access to Securities and Exchange Commission facilities.

Management Comments. OAS concurred with the recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased that OAS concurred with this recommendation.

Recommendation 14:

The Office of the Executive Director should require administrative officers in the regional offices, or designated points of contact, to enroll Personal Identity Verification cards in the Securities and Exchange Commission's physical access control system.

Management Comments. OED concurred with the recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased that OED concurred with this recommendation.

Recommendation 15:

The Office of the Executive Director should communicate to all Securities and Exchange Commission employees and contractors their responsibility to inform the appropriate regional office official that they have been issued a Personal Identity Verification card so that the card can be enrolled into the Securities and Exchange Commission's physical access control system.

Management Comments. OED concurred with the recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased that OED concurred with this recommendation.

Finding 5: OAS's Physical Security Branch Badging Policy Is Outdated and Does Not Include Procedures for Issuance and Revoking of Badges

OAS's Physical Security Branch does not have current policies and procedures for issuing and revoking badges or for requiring the use of the PIV credentials as the common means of authentication for access to SEC facilities and information systems. As a result, SEC employees and contractors could obtain access to SEC facilities beyond their separation date and also may be unaware of the right to appeal a decision denying or revoking their credentials.

OMB Circular A-123 states, "Management controls are the organization, policies, and procedures used to reasonably ensure that: (i) programs achieve their intended results; (ii) resources are used consistent with agency mission; (iii) programs and resources are protected from waste, fraud, and mismanagement; (iv) laws and regulations are followed; and (v) reliable and timely information is obtained, maintained, reported and used for decision making."[51]

FIPS 201-1 provides that an agency's PIV implementation must include "a revocation process . . . such that expired or invalidated credentials are swiftly revoked."[52] Further, FIPS 201-1 states, "The PIV credential shall be revoked if the results of the investigation so justify."[53] In addition, FIPS 201-1 requires

[51] The Office of Management and Budget's, Circular A-123, To the Heads of Executive Departments and Establishments; From: Alice M. Rivlin, Director; Subject Management Accountability and Control; Revised June 21, 1995; http://www.whitehouse.gov/omb/circulars_a123/ (Accessed on 02/03/2011).
[52] FIPS 201-1, p. 5, http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf.
[53] FIPS 201-1, p. 6, http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf.

agencies to "[m]aintain appeals procedures for those who are denied a credential or whose credentials are revoked." [54]

In addition, M-05-24 requires agencies, prior to identification issuance, to "[d]evelop, implement and post in multiple locations (e.g., agency intranet site, human resource offices, regional offices, provide at contractor orientation, etc.) [the] department's or agency's … appeals procedures for those denied identification or whose identification credentials are revoked…."[55]

In addition, OMB Memorandum M-11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors,*[56] states that "each agency should develop and issue an implementation policy, by March 31, 2011, 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." Based on our review of the SEC's policies and procedures, we determined that the agency has not developed and issued an implementation policy that requires the use of the PIV credentials as the common means of authentication for access to the SEC's facilities, networks, and information systems.

Further, GSA's *PIV Card Issuer Operations Plan* states in Section 4.1.3, Expiration Date Requirements, that "All credentials issued by MSO [GSA's Managed Service Office] must have an expiration date printed on the card. The expiration date for all credentials must be 5 years or less from the date of issuance. The expiration date of Foreign Nationals cannot exceed the expiration date of their INS documents (green card, work permit, etc.)."[57]

We found that the Physical Security Branch does not have formal, approved operating procedures. We were informed by Physical Security Branch staff that the operating procedures were in draft and are currently under internal review.

Additionally, we determined that the SEC's existing badging policy, SECR 5-2, *Identification Cards, Press Passes and Proximity Access Control Cards*,[58] is outdated and does not reflect the SEC's current badging policies and procedures or identify the types of badges that are issued. The existing badging policy does not include policies or procedures for (1) the various badge types that the SEC issues (including visitor and PIV badges), (2) revoking badges, or (3) appealing

[54] FIPS 201-1, p. 7, http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf.
[55] M-05-24, p. 9, Section 6.F, http://www.whitehouse.gov/omb/memoranda/fy2005/m05-24.pdf.
[56] OMB Memorandum M-11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*, February 3, 2011, http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf.
[57] GSA *USAccess PIV Card Issuer Operations* Plan, Version 1.0, CM # GSA-DI-0000129-1.4.0, August 1, 2007, Section 4.1.3, p. 80.
[58] SECR 5-2, *Identification Cards, Press Passes and Proximity Access Control Cards*, November 8, 1999, http://insider.sec.gov/policies_procedures/admin_regulations/r5-2.html.

revocation of badges.[59] In addition, the existing badging policy is not consistent with the SEC's current informal policies and procedures for issuance of badges. For example, SECR 5-2 provides that regular SEC identification cards are valid for three years.[60] However, Physical Security Branch staff informed us that its normal protocol is to issue a badge for two years from the date of issuance, and that the expiration date of the badge is not always consistent with the termination date requested by the Administrative Office or Designee on the *Identification/Access Control Card Worksheet*. The *Identification/Access Control Card Worksheet* is used by the Physical Security Branch to create badges for employees and contractors. In addition, we found that PIV credentials are issued with a standard five-year expiration date and, in some cases, have exceeded the contractor end-dates and could potentially exceed the expiration dates of INS documents (e.g., green card, work permit) for foreign nationals.

We also reviewed SECR 5-2[61] to determine if the SEC's appeals procedures for individuals who are denied identification and its revocation process for expired or invalidated credentials were appropriately documented and posted to the SEC's intranet site. We found that SECR 5-2 does not include the SEC's appeal procedures for individuals whose credentials were denied or revoked.

We also obtained a physical access control log report from the SEC's physical access control system (PACS), on September 7, 2010. After reviewing the PACS log, we found that there were multiple instances where employees or contractors were issued and are in possession of two types of badges that permit physical access (1) a PIV badge (referred to in the log as PIV II Template) and (2) a SEC badge (referred to in the log as Default Template).

During an interview with OAS staff, we were informed that it is OAS's expectation that the HSPD-12 badges will be used as the primary physical access badge for employees and contractors requiring physical access to SEC facilities for more than six months. Although OAS indicated that the HSPD-12 badge will be the primary physical access badge, we were informed that OAS determined that it would allow the currently issued SEC badges to expire in lieu of revoking them from current users (employees and contractors). In addition, in an interview with Physical Security Branch staff, we were informed that the Physical Security Branch determined that it would not revoke SEC badges for individuals who have been issued HSPD-12 badges, because the Physical Security Branch felt that deactivating SEC-issued badges would "unnerve" employees and contractors, who prefer the SEC-issued badge over HSPD-12 badge.

[59] The SEC OIG issued Report of Investigation No. OIG-544, *OIT Contract Employees Given Access to SEC Buildings and Computer Systems for Several Weeks Before Background Investigation Clearance,* on January 20, 2011. The Report of Investigation found that the Physical Security Branch has no written policy available on when visitor badges are to be issued.
[60] SECR 5-2, Section 2.a(3), http://insider.sec.gov/policies_procedures/admin_regulations/r5-2.html.
[61] SECR 5-2, Section A.2.a(3), http://insider.sec.gov/policies_procedures/admin_regulations/r5-2.html.

As previously mentioned, the OIG sent a survey to administrative officers or other designated persons in the SEC's 11 regional offices to obtain an understanding of the regional offices' badging practices. Our survey asked, "When an SEC employee is no longer employed at the SEC (retires, quits, is terminated, transfers to a job outside of the SEC, etc.), identify who obtains the employees badge." The survey respondents answered as follows:

- 16.7 percent – "I obtain the badge and retain it in my office desk/cabinet or in a secured desk/cabinet."
- 16.7 percent – "I obtain the badge and return it to the SEC's badging office."
- 16.7 percent – "I obtain the badge and return it to the SEC's OHR, Personnel Security Branch."
- 8.3 percent – "I obtain the badge and shred it, put it in a recycling bin, or put it in a trash receptacle."
- 8.3 percent – "I do not know."
- 33.3 percent – Other.

Thus, our survey indicated that there were widely varying practices among the regional offices for the proper disposition of the badges of employees who have separated from the SEC. We noted that SECR 5-2 states that in the Regional and District Offices, the Administrative Contact or Staffing Assistant should destroy the employee's regular identification card or special credential by cutting it into pieces and documenting the date of destruction in a logbook.[62] However, this policy was issued in November 1999 and may no longer reflect the proper procedures for disposition of the badges of separated SEC employees.

In addition, we surveyed administrative officers or other designated persons in the regional offices about the actions they take when a contractor separates, and 91 percent of the respondents indicated that they collect the badges. We noted that SECR 5-2 does not specify any procedure for handling the badges of separated contractors in the regional offices.[63]

We also surveyed contracting officials, including Contracting Officers (CO), Contract Specialists, COTRs, and IAOs across the Commission regarding what happens to contractors' badges when they separate or when their period of performance ends. Overall, 87 of 196 contracting officials responded to the survey; however, only 76 of the respondents completed the survey. In response to the question, "When a contractor is no longer assigned to an SEC contract (e.g., separation, termination, removal), or when the contract's period of performance ends, identify the disposition of the SEC badge," survey respondents stated the following:

[62] SECR 5-2, Section 10.c(3), http://insider.sec.gov/policies_procedures/admin_regulations/r5-2.html.
[63] SECR 5-2, Section 10.c, http://insider.sec.gov/policies_procedures/admin_regulations/r5-2.html.

- 23.4 percent – The badge is returned to the SEC's badging office.
- 26 percent – Did not know the disposition of the badge.
- 7.8 percent – The badge is taken by the CO, COTR, or IAO.
- 6.5 percent – The badge is taken to the OHR Personnel Security Branch.
- 36.4 percent – Other.

According to the procedures outlined in SECR 5-2, contractors are required to turn in their identification cards to their COTR upon termination of the contract, employment, etc.[64] However, this policy does not provide guidance to the COTRs on their responsibilities for handling badges once the contractor has been terminated or the contract's period of performance has ended. Additionally, we were unable to locate any policy or procedure that specified how COTRs should handle badges once they have received them from contractors.

Based on the results of both of our surveys, we found that the regional offices and contracting officials are not consistently obtaining the badges of employees and contractors who are separating from the SEC and there is no consistent practice for handling the badges of separated employees and contractors. Further, we found that the SEC does not have any updated policies and procedures for revoking PIV badges. In addition, we were unable to locate any references to the SEC's appeal procedures for individuals who have had credentials denied or revoked.

As a result, SEC employees and contractors could obtain physical access to SEC facilities beyond their separation date. In addition, employees and contractors who are denied credentials or whose credentials are revoked may be unaware of their rights to due process and their ability to appeal the initial decision.

Recommendation 16:

The Office of the Executive Director should develop and implement a policy requiring the Personal Identity Verification badge to be used as a common and primary means of authentication for physical and logical access.

Management Comments. OED concurred with the recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased OED concurred with this recommendation.

[64] SECR 5-2, Sections 10.a(3) and 10.b(2), http://insider.sec.gov/policies_procedures/admin_regulations/r5-2.html. We note that these requirements only pertain to the Commission's former Headquarters building (Judiciary Plaza) and the Operations Center/ Annex, and are thus outdated.

Recommendation 17:

The Office of Administrative Services should revise and update its *Identification Cards, Press Passes and Proximity Access Control Cards* policy to reflect current and proper practices for issuance and revocation of badges, including Personal Identify Verification cards, to Securities and Exchange Commission employees and contractors at all Commission facilities and post the revised policy on the Commission's intranet site. In addition, the Office of Administrative Services should communicate the new policy to all employees and contracting officials.

Management Comments. OAS concurred with the recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased that OAS concurred with this recommendation.

Recommendation 18:

The Office of Administrative Services should develop and implement a plan to systematically revoke all Commission-issued badges for all employees and contractors who have been issued Personal Identify Verification badges and ensure the plan is implemented within six months of the date this report is issued.

Management Comments. OAS concurred with the recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased that OAS concurred with this recommendation.

Recommendation 19:

The Office of Human Resources should develop, implement, and post in multiple locations (agency intranet site, human resource offices, regional offices, contractor orientation, etc.) its appeals procedures for individuals who are denied credentials or whose credentials are revoked.

Management Comments. OHR concurred with the recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased that OHR concurred with this recommendation.

Finding 6: OHR's Personnel Security Branch Does Not Have Policies and Procedures for Adjudicating Foreign Nationals

> OHR's Personnel Security Branch does not have policies or procedures specific to adjudicating foreign nationals. As a result, the Personnel Security Branch may be inconsistently applying suitability guidelines to foreign nationals.

M-05-24 provides, "Since Foreign National employees and contractors may not have lived in the United States long enough for a NACI [National Agency Check with Inquiries] to be meaningful, agencies should conduct an equivalent investigation, consistent with your existing policy."[65] As described in the OPM *Suitability Processing Handbook*, a NACI investigation consists of searches of the following records: OPM's Security/Suitability Investigations Index (SII); an FBI Name Check and National Criminal History fingerprint check; the Department of Defense Clearance & Investigations Index; and other records covering specific areas of an individual's background. In addition, a NACI includes written inquires to references, employers, places of education and residence, and other record sources covering specific areas of an individual's background.[66]

The OPM *Suitability Processing Handbook* further states, "Materials to be retained for an OPM Appraisal. The following information pertaining to suitability adjudications will be maintained for OPM review: The agency's suitability regulations and/or instructions."[67] We found that SEC's OHR Personnel Security Branch adopted OPM's *Suitability Processing Handbook* as its primary guide for all suitability investigations as a result of an OIG recommendation contained in the 2008 *Background Investigations* inspection report.[68] However, based on our review of OPM's *Suitability Processing Handbook,* we determined that the handbook does not have procedures or policies for adjudicating Foreign Nationals.

In addition, although the Personnel Security Branch had previously informed the OIG that procedures for processing foreign nationals participating in the SEC's Law Student Observer program had been completed, it did not produce any such procedures. Therefore, we were unable to confirm that procedures for processing foreign national student observers were developed or issued.

As a result, personnel security activities with respect to foreign nationals may not be consistently followed or conducted in accordance with federal requirements.

---

[65] M-05-24, page 5, http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf.
[66] OPM *Suitability Processing Handbook,* September 2008, p. 3.
[67] OPM *Suitability Processing Handbook,* September 2008, p. XI-3, Section D.
[68] OIG *Background Investigations* Inspection Report No. 434, March 28, 2008, Recommendation A.

In addition, background investigations of foreign nationals may be adjudicated using record searches that are not equivalent to a NACI.

Recommendation 20:

The Office of Human Resources should develop internal policies and procedures for suitability determinations for foreign nationals.

Management Comments. OHR concurred with the recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased that OHR concurred with this recommendation.

Finding 7: OIT is Unaware of the Number of Devices in Its Inventory That Would Physically Permit Authentication of PIV Cardholders Accessing SEC's Logical Information Resources

> OIT's asset inventory does not account for keyboards and lacks detail to easily verify laptops that have physical features (i.e., card readers) to permit authentication of PIV credentials. As a result, there is a risk that OIT will purchase additional equipment to support the use of PIV credentials for logical access when it already has the equipment in its inventory.

HSPD-12 requires that by October 2005, eight months after promulgation of the Standard, the SEC should require the use of the PIV credential for gaining logical access to federally controlled information systems.[69]

In our report *2010 Annual FISMA Executive Summary Report*, Report No. 489, we found that OIT has not completed logical access integrations of PIV credentials. As a result, we recommended that OIT complete the logical access integration of the HSPD-12 cards by no later than December 2011, as the SEC had reported to OMB on December 31, 2010.

In addition to the above-mentioned finding and recommendation, we found that OIT has deployed keyboards and laptops that have card readers to employees and contractors without tracking which specific devices actually have card readers. Furthermore, in the survey we issued to the regional offices, 9 of 11

[69] HSPD-12, http://csrc.nist.gov/drivers/documents/Presidential-Directive-Hspd-12.html.

regional office representatives responded that desktops have not been deployed to support logical access to the SEC's network using HSPD-12 badges.

OIT informed us that it has not tracked the number of keyboards containing card readers because it has classified keyboards as a consumable device[70] and consequently has not maintained an inventory of them. Based on our audit, we believe this information should be tracked notwithstanding the classification of keyboards as a consumable device because it is important for OIT to know whether keyboards contain card readers to avoid unnecessary expenditures. In addition, OIT's asset inventory does not contain detailed information regarding which laptops have card readers installed. As a result, the SEC is not aware of the hardware in its inventory that can be used for authentication once the SEC deploys identity management software throughout the enterprise to support the logical access requirements of HSPD-12. Without conducting an inventory of all keyboards and laptops with card readers, OIT may unnecessarily purchase new keyboards and laptops with card readers or external card readers. By identifying the keyboards and laptops that have card readers, OIT will be able to save the agency the unnecessary costs of purchasing additional equipment.

Recommendation 21:

The Office of Information Technology should immediately conduct an audit of its inventory to identify and track all keyboards and laptops that contain card readers.

Management Comments. OIT concurred with the recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased that OIT concurred with this recommendation.

Recommendation 22:

The Office of Information Technology should promptly deploy appropriate technology (e.g., laptops with internal card readers, keyboards with card readers, or external card readers) to employees and contractors who do not have card readers.

Management Comments. OIT concurred with the recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased that OIT concurred with this recommendation.

[70] OIT considers a "consumable device" to include a piece of hardware such as a keyboard or a mouse that costs less than $250 and is not a storage device (e.g., an external hard drive).

Finding 8: OIT Has Unnecessarily Employed Two Full-Time Registrars

> OIT employs two full-time registrars; however, based on the average number of transactions processed per day, the SEC requires only one part-time registrar.

As described in FIPS 201-1, a registrar (also referred to as a PIV registrar) is responsible for identity proofing of applicants and ensuring the successful completion of background checks. In addition, the registrar provides the final approval for the issuance of a PIV credential to the applicant.[71]

At the onset of HSPD-12 implementation, OIT decided to use a shared service provider, GSA, for its implementation of HSPD-12. GSA has provided the SEC with an identity management and credentialing solution for end-to-end services, including proofing and registering applicants, issuing credentials, and managing the lifecycle of credentials.

GSA Managed Service Offices (MSOs) are conveniently located throughout the United States and have multiple locations in the District of Columbia (D.C.) metropolitan area. Although MSOs are located throughout the D.C. metropolitan area, GSA established an MSO office at SEC headquarters due to its proximity to Union Station. GSA provided the enrollment and activation stations at no cost to the SEC, but with the stipulation that the MSO at the SEC would be a shared center, meaning it would be available to both SEC employees and contractors and non-SEC employees and contractors.

In addition, for a limited period of time, GSA provided the SEC with one registrar at no cost. The SEC agreed to house the MSO at headquarters to afford SEC employees and contractors the convenience of registering and activating credentials without having to go off-site. However, SEC employees and contractors who work in the regional offices would be required to register and activate credentials at their local MSO. While the SEC initially did not pay for the registrar located at SEC headquarters, beginning in June 2009, as a result of delays in the SEC's implementation of the HSPD-12 initiative, the SEC began paying for the headquarters registrar. The SEC is paying approximately $72,000 annually for a full-time register at its headquarters. In June 2010, at the request of OIT, the SEC opened a second MSO at the Operations Center on the premise that it would be less costly to pay for an on-site station than to have contractors spend several hours going back and forth between the Operations Center and headquarters to register and activate their credentials. The MSO located at the Operations Center is also operated by a full-time register, which costs the

[71] FIPS 201-1, page 52, http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf.

Commission an additional $72,000[72] annually. The Operations Center MSO is only for the use of SEC employees and contractors and is not a shared center.

Based upon interviews and a review of the registrar schedule, we determined that for each transaction to register or activate an HSPD-12 badge, the registrar is allocated 15 minutes to complete the transaction. The SEC's HSPD-12 agency role administrator provided the number of transactions that occurred at both MSO offices located in SEC facilities, at headquarters and the Operations Center, from May 2010 through November 2010. Based on the data provided by the SEC, we determined that the MSOs, on behalf of the SEC, processed a total of 1,215 transactions — 1,029 at headquarters (an average of 147 transactions per month and 7 transactions per day)[73] and 186 at the Operations Center (an average of 27 transactions per month and 1 transaction per day).[74] See Table 4 below for a breakdown of the number of transactions by month.

Table 4: Number of Transactions Processed between May 2010 and November 2010 by Registrars

Month	Headquarters	Operations Center
May 2010	113	44
June 2010	136	17
July 2010	185	14
August 2010	141	37
September 2010	199	20
October 2010	132	37
November 2010	123	17
Total	**1,029**	**186**

Source: OIG-generated.

Based on our analysis of the transaction data, we determined that the register at headquarters is processing an average of only seven transactions in an eight-hour workday, and the registrar at the Operations Center is processing only one transaction in an eight-hour workday. Yet we determined from a review of the GSA scheduling timeframes that it takes approximately 15 minutes to complete a transaction. Therefore, the registrar at headquarters is working on processing transactions for an average of only one hour and 45 minutes per day,[75] and the

[72] This number, $72,000, is an approximation not an exact figure.
[73] We calculated the average number of transactions per month of 147 by dividing the total number transactions at Headquarters of 1,029 by seven months. Based on 20 working days per month and average transactions per month of 147, we calculated the average transactions per day to be 7.35, and rounded to 7 transactions per day.
[74] We calculated the average number of transactions per month of 27 by dividing the total number of transactions at the Operations Center of 186 by seven months and rounding up. Based on 20 working days per month and the average transactions per month of 27, we calculated the average transactions per day to be 1.35, rounded to one transaction per day.
[75] Based on the average number of transactions per day at Headquarters of seven, multiplied by the time allotted for a transaction of 15 minutes, divided by 60 minutes (number of minutes in an hour), the average

registrar at the Operations Center is working on processing transactions for an average of only 15 minutes per day.[76] Combined, the registrars are spending an average of only two hours per day processing transactions. The SEC could realize a significant cost savings by eliminating one full-time registrar and making the other registrar part-time,[77] for a total cost savings of $108,000 annually. This $108,000 represents the cost the OIG identified that is considered cost savings and/or funds put to better use. See Table 5 in Appendix V for cost savings.

Delays in the SEC's implementation of the HSPD-12 directive caused the SEC to fail to realize the benefits of using a full-time registrar at no cost to the Commission. If the SEC had achieved the time requirements set forth in the implementation standard, the agency would have issued badges to all employees and contractors and integrated the credentials into their physical and logical access controls systems by October 2008. As a result of implementation delays, OIT has had to pay for the cost of the registrar located at headquarters since June 2009.

In addition, the SEC did not conduct an analysis before employing a second full-time registrar or consider alternative options, such as splitting the time of the existing registrar between both facilities or hiring a part-time registrar to work at the Operations Center. While OIT represented that managers determined it would be cheaper, they were unable to provide a formal analysis. As a result, the SEC has expended a total of approximately $144,000[78] which would not have had to be spent if the Commission had implemented HSPD-12 within the required timeframes.[79] Moreover, by not conducting an analysis prior to employing an additional full-time registrar, the SEC has expended unnecessary costs to employ two full-time registrars when, based on an eight-hour workday, the two registrars combined are spending an average of only two hours per day processing transactions.

---

amount of time used to process transactions in an eight-hour work day is 1.75 hours or one hour and 45 minutes.

[76] Based on the average number of transactions per day at the Operations Center of one multiplied by the time allotted for a transaction of 15 minutes, divided by 60 minutes (number of minutes in an hour), the average amount of time used to process transactions in an eight-hour workday is 0.25 hours, or 15 minutes.

[77] The annual cost of one registrar is approximately $72,000 (eight-hour work day), and the cost of a registrar working a four-hour workday equals approximately $36,000.

[78] The total expended to employ a registrar located at Headquarters is the annual cost of $72,000 multiplied by 1.5 years (June 2009 – December 2010), which equals $108,000. The total cost expended for the registrar located at the Operations Center is the annual cost of $72,000 multiplied by .5 year (June 2010 – December 2010), which is $36,000. Therefore, the total cost of employing registrars at Headquarters and the Operations Center from June 2009 through December 2010 was approximately $144,000.

[79] The requisite timeframes included verification and/or completion of background investigation for all current employees and contractors, except for employees with more than 25 years of federal service by October 27, 2007, and completion of background investigations for all employees with more than 15 years of federal service by October 27, 2008. M-05-24, p. 6, http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf.

Recommendation 23:

The Office of Information Technology should eliminate one-full time registrar and split the time of the other full-time registrar between the Operations Center and headquarters locations.

Management Comments. OIT concurred with the recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased that OIT concurred with this recommendation.

Finding 9: OAS's Physical Security Branch Is Not Maintaining Visitor Logs in Accordance with the Applicable Record Retention Policies

OAS's Physical Security Branch is not maintaining visitor record logs in accordance with the National Archives and Records Administration's (NARA) two-year general records schedule. As a result, the Physical Security Branch is unable to analyze visitor logs to determine if visitors are accessing the agency inappropriately (i.e., circumventing the badging process for persons requiring access longer than six months).

The Physical Security Branch maintains visitor control logs (referred to as the e-visitor, or the EZLobby or eAdvance system) for 90 days. The EZLobby system is used by the Physical Security Branch staff at headquarters and the Operations Center to capture detailed visitor information and issue badges. The EZLobby system allows the Physical Security Branch personnel at headquarters and the Operations Center to share visitor information, and it allows SEC employees to use a web-based tool (eAdvance) to pre-register guests and receive e-mail notification when visitors check in. Finally, EZLobby allows OAS managers to perform analysis of and generate reports on visitor data.[80]

NARA's General Records Schedule 18, Security and Protective Services Records, Section 17, *Visitor Control Files,* states, "Registers or logs used to record names of outside contractors, service personnel, visitors, employees admitted to areas, and reports on automobiles and passengers. (a) For areas under maximum security. Destroy 5 years after final entry or 5 years after date of document, as appropriate. (b) For other areas. Destroy 2 years after final entry

[80] List of SEC Systems. http://intranet.sec.gov/knowledge_center/SEC%20Systems/index.html.

or 2 years after date of document, as appropriate."[81] The Physical Security Branch informed us that EZLobby logs are maintained for 90 days. On November 16, 2010, the Physical Security Branch provided the OIG with a copy of data retrieved from OAS's e-Visitor (also called EZLobby or eAdvance) system. After reviewing the data output "check in" and "check out" dates, we confirmed that the e-Visitor log provided by the Physical Security Branch was for only a 90-day period (August 15, 2010, to November 16, 2010). Retention of visitor logs for 90 days does not satisfy the two-year retention requirement set forth by the NARA General Records Schedule for Security and Protective Services Records.

Further, an initial review of data output from EZlobby revealed that some names appeared multiple times. As a result, we sorted the data output by last name and then first name using Microsoft Excel. Upon completion of the data sort, we reviewed and analyzed the results to identify individuals who appeared to have visited the SEC on a frequent and sometimes daily basis between August 15, 2010, and November 16, 2010. Of the 16,766 entries in data output from EZLobby, approximately 107 visitors accessed the SEC almost daily during the time period examined. The *Security Reminder* contained in the SEC's eAdvance Visitor Pre-Registration System states, "EZLobby badges are temporary badges issued to SEC visitors or individuals required to be on site for one day. An EZLobby badge requires an escort at all times. The EZLobby badge is not to be used in lieu of, or while your employee is waiting for issuance of a permanent badge."

Due to the lack of data for a period beyond 90 days, we are unable to determine if visitors were obtaining access for a period greater than six months. However, we were able to ascertain, based upon the frequency with which their names appeared in the data output, that approximately 107 visitors did not appear to comply with the *Security Reminder*, which indicates that temporary badges are issued to visitors for one day and should not be used in lieu of a permanent badge. Based on our review and analysis, we determined that the SEC is potentially permitting access to visitors through the issuance of daily visitor passes in circumvention of the SEC's HSPD-12 badging process.

In addition, M-05-24 states that agencies who employ temporary personnel should "[d]evelop agency-specific visitor policies (as appropriate) for occasional visitors."[82] On January 20, 2011, the OIG issued Report of Investigation *OIT Contract Employees Given Access to SEC Buildings and Computer Systems for Several Weeks Before Background Investigation Clearance,* Report No. OIG-544. The Report of Investigation determined that the Physical Security Branch had no written policy for when visitor badges were to be issued and recommended the issuance of a written policy on the proper issuance and

[81] NARA General Records Schedule 18, Security and Protective Services Records**,** Transmittal No. 22, April 2010, http://www.archives.gov/records-mgmt/grs/grs18.html.
[82] M-05-24, page 11, http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf.

documentation of visitor badges, specifically noting that visitor badges cannot be issued in lieu of, or while awaiting, a permanent official SEC badge.

In summary, our audit found that the Physical Security Branch is maintaining visitor logs for only 90 days, in violation of the NARA records retention requirement. As a consequence, the Physical Security Branch is unable to review visitor logs for a sufficient period of time to determine if visitors are accessing the agency inappropriately (i.e., on a daily basis or in lieu of a permanent badge). Moreover, OAS does not document the results of its analysis of visitor data. Due to these deficiencies, the Physical Security Branch is unable to ensure that individuals are not circumventing the SEC's HSPD-12 badging process by repeatedly obtaining visitor badges.

Recommendation 24:

The Office of Administrative Services should retain visitor control logs for a period not less than two years after final entry or two years after date of document in accordance with the National Archives and Records Administration's General Records Schedule.

Management Comments. OAS concurred with the recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased that OAS concurred with this recommendation.

Recommendation 25:

The Office of Administrative Services should perform periodic analysis of visitor data to ensure that visitors are not circumventing the HSPD-12 requirements.

Management Comments. OAS concurred with the recommendation. See Appendix VI for management's full comments.

OIG Analysis. We are pleased that OAS concurred with this recommendation.

Acronyms/Abbreviations

CAS	Civilian Applicant System
CFR	Code of Federal Regulations
COTR	Contracting Officer's Technical Representative
DNI	Director of National Intelligence
ED	Executive Director
FBI	Federal Bureau of Investigations
FIPS	Federal Information Processing Standards
GSA	General Services Administration
HSPD-12	Homeland Security Presidential Directive
IAO	Inspection Acceptable Officer
MSO	Managed Service Office
NACI	National Agency Check with Inquiries
NIST	National Institute of Standards and Technology
OAS	Office of Administrative Services
OED	Office of the Executive Director
OHR	Office of Human Resources
OIG	Office of Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PACS	Physical Access Control System
PIN	Personal Identification Number
PIV	Personal Identity Verification
SEC	U.S. Securities and Exchange Commission

Scope and Methodology

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 objectives. We determined that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Scope. We obtained information from OHR, OAS, and OIT on the SEC's implementation and compliance with the HSPD-12. In addition, we surveyed the SEC's 11 regional offices' administrative officers to obtain an understanding if the agency has consistently implemented HSPD-12 across the board. Further, to obtain an understanding of the training and/or guidance received by contracting officials such as CO's, Contract Specialists, COTRs, and IAOs on the SEC's HSPD-12 badging policies and procedures, we conducted a separate survey.

We conducted our fieldwork from August 2010 to February 2011. We reviewed documentation pertaining to the SEC's implementation and compliance with HSPD-12 for calendar years 2007 through 2010.

Methodology. To meet the audit objective to determine if the SEC is fully compliant with HSPD-12 and implementing standards and guidance, we reviewed the *Implementation of Homeland Security Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*, OMB memoranda and circulars, NIST, and Federal Information Processing Standards governing HSPD-12, and other governing guidance to obtain an understanding of the agency's requirements for implementing HSPD-12. We developed and issued two separate surveys to specific SEC staff as follows: (1) one to the SEC's regional office staff who are responsible for badging or the administrative functions and (2) one to persons having responsibility for overseeing contractors such as IOAs, Contracting Officers, COTRs, and Contracting Specialists. The surveys included questions to determine if badges were properly seized upon an SEC contractor's termination from the SEC or when the period of performance on a contract has ended. The surveys were further used to determine if consistent practices exist for seizing badges when a contractor is terminated from the SEC or when a contractor's period of performance has ended. We also assessed whether the SEC met the OMB guidance timeframes. In addition, we conducted interviews with staff in the OHR's Personnel Security Branch, OIT, and the OAS's Physical Security Office and Contracting Office to discuss their responsibilities related to the HSPD-12 directive.

To meet the audit objective for evaluating whether the SEC has adequate controls and the necessary processes and procedures to (1) perform background investigations, (2) adjudicate results, and (3) issue credentials, we reviewed documentation that supported the implementation of prior OIG recommendations to determine if the recommendations were properly closed. We further reviewed the SEC's internal policies and procedures, operating procedures, and manuals that apply to the HSPD-12 directive. Additionally, we conducted interviews with staff in OHR and OED to discuss their procedures for performing background investigations, adjudicating results, and issuing credentials.

To meet the audit objective for evaluating the roles and responsibilities for the HSPD-12 initiative among the various offices involved in the process, including OAS, OHR, and OIT, we conducted interviews with staff in OHR's Personnel Security Branch, OIT, and OAS's Physical Security Office and Contracting Office to discuss their responsibilities related to the HSPD-12 directive. In addition, the survey we developed included questions to determine if staff in the SEC regional offices that are responsible for badging and persons having responsibility for overseeing contractors understand their roles and responsibilities for the HSPD-12 initiative, such as enrolling badges into the SEC's physical access control system.

To meet the audit objective for assessing compliance with HSPD-12 and determining whether all the necessary equipment was purchased to implement HSPD-12 throughout the SEC, we reviewed the results from the *2010 Annual FISMA Executive Summary Report*, Report No. 489 and conducted interviews with OIT and OAS staff. Additionally, we developed and issued a survey to the SEC's regional office staff who are responsible for badging or the administrative functions. The survey also included questions to determine if needed equipment had been purchased to implement HSPD-12 for both physical and logical access.

To meet the audit objective for evaluating whether the HSPD-12 processes and procedures were consistently applied throughout the SEC (i.e. at headquarters and the regional offices), the survey we issued included questions to pertaining to whether HSPD-12 processes and procedures were consistently applied for badge issuance and enrolling badges into the SEC's physical access control system. The survey further included questions regarding whether equipment was deployed to implement HSPD-12 initiative for both physical and logical access, and procedures for revoking badges are consistent.

Sampling. We identified a population (universe) of "all" badges that were issued to SEC staff and contractors at its headquarters and regional offices from FY 2007 through FY 2010. Our universe was determined by (1) reviewing the SEC's physical access control system, Diebold Hirsh; (2) reviewing the SEC's visitor access control system; and (3) obtaining and reviewing a list of contractors that was provided by OAS's Contracting Office.

Based on the universe of badges, we developed a testing strategy and verified that the SEC's employees and contractors received an SEC badge and/or HSPD-12 badge based on the Commission's policies and procedures. From the SEC's physical access control log provided by the Physical Security Branch, we judgmentally selected visitors who visited the SEC's headquarters at least three time in a week and up to five times in a week over a 90-day period.

In addition, we judgmentally selected a sample of four contracts that had an effective date between calendar year 2008 and calendar year 2010 to determined if the contracts contained Federal Acquisition Regulation clause 52.204.9 as required by OMB Memorandum M-05.24, Office of Management and Budget (OMB) Memorandum M-05-24, dated August 5, 2005, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*.

Prior OIG Reports and Memoranda. The following four prior OIG reports and memoranda are relevant to this audit:

- OIG Report of Investigation No. OIG-544, *OIT Contract Employees Given Access to SEC Buildings and Computer Systems for Several Weeks Before Background Investigation Clearance,* issued on January 20, 2011, which contained four recommendations to strengthen management controls pertaining to contractor access to SEC facilities and information systems.
- OIG Inspection Report No. 434, *Background Investigations,* issued on March 28, 2008, which contained nine recommendations to strengthen management controls over OHR's background investigation program.
- OIG Investigative Memorandum No. G-444, *Law Student Observer Program,* issued on June 29, 2006, which contained three recommendations to strengthen management controls over OHR's background investigation program, specifically for interns selected through the SEC's Law Student Observer Program.
- OIG Audit Memorandum No. 39, *Operations Center Building Security*, issued on July 14, 2005, which contained three recommendations to strengthen management controls over building security at the SEC Operations Center located in Alexandria, Virginia.

Internal Controls. The GAO *Government Auditing Standards*, effective January 1, 2008, includes the requirement to understand internal controls that are significant within the context of the audit's objectives. The revised standards indirectly refer to the Internal Control – Integrated Framework (COSO Report), published by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and *GAO Standards for Internal Controls in the Federal Government*. The COSO report provides the framework for organizations to design, implement, and evaluate controls that will facilitate compliance with

federal laws, regulations, and program compliance requirements. OIG used the COSO framework to measure the SEC's control activities. Specifically, we reviewed the auditee's internal controls as they pertained to the audit objectives and applied the COSO framework's five components to assess whether the SEC's controls were adequate and to determine if the SEC had the needed processes and procedures in place to:

- perform background investigations,
- adjudicate results, and
- issue credentials.

Finally, we assessed the SEC's controls in determining the roles and responsibilities of the offices that were involved in implementing the HSPD-12 directive and we evaluated whether HSPD-12 processes and procedures are consistently applied throughout the agency.

Use of Computer-Processed Data. We did not assess the reliability of the GSA's USAccess application, SEC's physical access control system (HIRSH), SEC's visitor badging system (EZLobby/eVisitor), the survey tool (Survey Monkey), and OMB's E-Government and Information Technology website (for HSPD-12 Implementation Status Reports) because these applications and systems did not pertain to our audit objectives. Further, we did not perform any tests on the general or application controls over these automated systems, as this was not in our scope. The information that was retrieved from these systems, as well as the requested information that was provided to us was sufficient, reliable, and adequate to use to meet our stated objectives. In addition, we reviewed the following computer processed data (e.g., Excel spreadsheets) that OHR and OAS staff provided OIG:

- list of current contractors,
- list of employees with no investigation or noncompliant investigation over 15 years, and
- list of employees with an investigation over 15 years who were grandfathered.

Criteria

Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*. This directive established the requirement for a mandatory, government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and contractor employees assigned to government contracts in order to enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy.

Office of Management and Budget (OMB) Memorandum M-05-24, August 5, 2005, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*. This memorandum provides implementing instructions for the HSPD-12 Directive and Federal Information Processing Standard 201.

Department of Commerce's Federal Information Processing Standard (FIPS) 201-1 – *Personal Identity Verification (PIV) of Federal Employees and Contractors.* Establishes the minimum requirements for a federal personal identity verification system (PIV-I) and detailed technical specifications of components and processes required for interoperability of PIV credentials (PIV-II).

SEC Administrative Regulations, *Identification Cards, Press Passes and Proximity Access Control Cards*, SECR5-2, November 8, 1999. This regulation prescribes policies, procedures, and standards that govern the Securities and Exchange Commission's (SEC) identification cards.

USA Access Program, *PIV Card Issuer Operations Plan*, Version 1.0, August 1, 2007, CM# GSA-DI-0000129-1.4.0. The PIV Card Issuer Operations Plan describes the operations and procedures at the MSO and agency levels, including the assignment of PIV roles and responsibilities.

NIST, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*, November 2008, Special Publication 800-116. This publication provides recommendations for the use of Personal Identity Verification credentials in physical access control systems.

Federal Acquisition Regulation (FAR) 52.204-9, Personal Identity Verification of Contractor Personnel. The FAR is the principal set of rules for federal acquisitions. It consists of regulations that govern the process through which the government acquires goods and services. As required by FIPS 201 and OMB M-05-24, contracts and solicitations that require contractors to have

routine physical access to a federally controlled facility or routine access to a federally controlled information system should contain this provision.

Executive Order 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information. This Executive Order provides the executive branch's policies and procedures relating to suitability, contractor employee fitness, eligibility to hold a sensitive position, access to federally controlled facilities and information systems, and eligibility for access to classified information. It provides that these policies and procedures are to be aligned using consistent standards to the extent possible, provide for reciprocal recognition, and ensure cost-effective, timely, and efficient protection of the national interest, while providing fair treatment to those upon whom the federal government relies to conduct the nation's business and protect national security.

List of Recommendations

Recommendation 1:

The Office of Human Resources should immediately prepare formal, documented plans for initiating background investigations for all current employees who do not have successfully adjudicated background investigations on record, commensurate with risk.

Recommendation 2:

The Office of Human Resources should immediately, but no later than 90 days after the issuance of this report, initiate background investigations for all current employees who do not have successfully adjudicated investigations on record, commensurate with risk.

Recommendation 3:

The Office of Administrative Services should identify and develop a consolidated list of all contractors who are employed by the Commission. In addition, the Office of Administrative Services should coordinate with the Contracting Officer's Technical Representatives and Inspection and Acceptance Officials to implement policies and procedures for ensuring that the list remains up to date.

Recommendation 4:

The Office of Administrative Services should provide the Office of Human Resources Personnel Security Branch with a copy of the up-to-date consolidated contractor list on a weekly basis.

Recommendation 5:

Upon receipt of the up-to-date consolidated contractor list, the Office of Human Resources Personnel Security Branch should determine which contractors do not have successfully adjudicated background investigations on record and develop a plan to begin the required background investigations immediately.

Recommendation 6:

Upon receipt of the up-to-date consolidated contractor list, the Office of Human Resources should ensure that accurate status reporting has been made to the Office of Management and Budget.

Recommendation 7:

The Office of Executive Director should discontinue adjudicating all eligibility determinations for access to classified information or holding a sensitive position until the Securities and Exchange Commission has received an appropriate delegation of authority to conduct such determinations from the Director of National Intelligence.

Recommendation 8:

The Office of Executive Director should identify all eligibility determinations for access to classified information or holding a sensitive position adjudicated by the Securities and Exchange Commission since June 30, 2008, and, upon receipt of authority from the Director of National Intelligence, conduct a quality control assessment to ensure that the determinations were conducted in accordance with the uniform policies and procedures developed by the Director of National Intelligence.

Recommendation 9:

The Office of Executive Director, upon receipt of authority from the Director of National Intelligence to make eligibility determinations for access to classified information or holding a sensitive position, should use the uniform policies and procedures developed by the Director of National Intelligence when making such determinations.

Recommendation 10:

The Office of Administrative Services should immediately discontinue making eligibility determinations for persons requiring temporary access to Securities and Exchange Commission facilities or information systems without proper authorization.

Recommendation 11:

The Office of Administrative Services should immediately provide the Office of Human Resources Personnel Security Branch with a list of all persons who have been provided or denied access based on the Physical Security Branch's risk assessments, as well as a copy of all fingerprints records, supporting documentation, and the results of the risk assessments.

Recommendation 12:

The Office of Human Resources, in coordination with the Office of Administrative Services, should develop policies and procedures for determining the eligibility of contractors and visitors and guests requiring temporary access to Securities and Exchange Commission facilities or information systems.

Recommendation 13:

The Office of Administrative Services should communicate to regional office staff its expectations for enrolling Personal Identity Verification credentials into their physical access control systems and using the Personal Identity Verification credential as the primary badge for physical access to Securities and Exchange Commission facilities.

Recommendation 14:

The Office of Administrative Services should require administrative officers in the regional offices, or designated points of contact, to enroll Personal Identity Verification cards in the Securities and Exchange Commission's physical access control system.

Recommendation 15:

The Office of the Executive Director should communicate to all Securities and Exchange Commission employees and contractors their responsibility to inform the appropriate regional office official that they have been issued a Personal Identity Verification card so that the card can be enrolled into the Securities and Exchange Commission physical access control system.

Recommendation 16:

The Office of the Executive Director should develop and implement a policy requiring the Personal Identity Verification badge to be used as a common and primary means of authentication for physical and logical access.

Recommendation 17:

The Office of Administrative Services should revise and update its *Identification Cards, Press Passes and Proximity Access Control Cards* policy to reflect current and proper practices for issuance and revocation of badges, including Personal Identity Verification cards, to Securities and Exchange Commission employees and contractors at all Commission facilities and post the revised policy on the Commission's intranet site. In addition, the Office of Administrative Services should communicate the new policy to all employees and contracting officials.

Recommendation 18:

The Office of Administrative Services should develop and implement a plan to systematically revoke all Commission-issued badges for all employees and contractors who have been issued Homeland Security Presidential Directive 12 badges and ensure that the plan is implemented no later than 6 months after the date this report is issued.

Recommendation 19:

The Office of Human Resources should develop, implement, and post in multiple locations (e.g., agency intranet site, human resources offices, regional offices, contractor orientation) its appeals procedures for individuals who are denied credentials or whose credentials are revoked.

Recommendation 20:

The Office of Human Resources should develop internal policies and procedures for suitability determinations for foreign nationals.

Recommendation 21:

The Office of Information Technology should immediately conduct an audit of its inventory to identify and track all keyboards and laptops that contain card readers.

Recommendation 22:

The Office of Information Technology should promptly deploy appropriate technology (e.g., laptops with internal card readers, keyboards with card readers, or external card readers) to employees and contractors who do not have card readers.

Recommendation 23:

The Office of Information Technology should eliminate one full-time registrar and split the time of the other full-time registrar between the Operations Center and headquarters locations.

Recommendation 24:

The Office of Administrative Services should retain visitor control logs for a period not less than two years after final entry or two years after date of document in accordance with the National Archives and Records Administration's General Records Schedule.

Recommendation 25:

The Office of Administrative Services should perform periodic analysis of visitor data to ensure that visitors are not circumventing the HSPD-12 requirements.

Schedule of Cost Savings

Table 5. Schedule of Cost Savings

SEC's Registrar Salaries	Cost Savings
Eliminate 1 full-time SEC registrar salary at $72,000/year	$72,000
Eliminate ½ full-time SEC registrar salary at $36,000/year	$36,000
Total	**$108,000**

Source: OIG-generated.

Management's Comments

MEMORANDUM

TO: H. David Kotz
Inspector General

FROM: Diego T. Ruiz,
Executive Director
Office of the Executive Director (OED)

Jeffrey A. Risinger
Associate Executive Director
Office of Human Resources (OHR)

DATE: March 28, 2011

SUBJECT: OED/OHR Joint Response to Report No. 481, *Draft Implementation of and Compliance with Homeland Security Presidential Directive 12*

This memorandum provides the OED and OHR response to OIG Report No. 481, dated March 10, 2011. The OIG report contains 12 recommendations directed to OED and OHR (recommendations 1, 2, 5, 6, 7, 8, 9, 12, 15, 16, 19, 20). The report's remaining recommendations, which are directed to the Office of Administrative Services and the Office of Information Technology, will be responded to in separate memorandums from those offices.

We concur with each of these 12 recommendations directed to our offices, and will take immediate action to develop a corrective action plan to address these recommendations.

We also want to provide additional management comments with respect to two specific recommendations:

Recommendation 7: The Office of Executive Director should discontinue adjudicating all eligibility determinations for access to classified information or holding a sensitive position until the Securities and Exchange Commission has received an appropriate delegation of authority to conduct such determinations from the Director of National Intelligence (DNI).

OED Response: OED concurs with this recommendation and has initiated contact with the DNI to obtain the necessary delegated adjudication authority. Should this process take longer than several weeks, even for an interim adjudication authority, we may be faced with the need to make adjudications of current investigations. The OED will work expeditiously to complete this recommendation and will keep the OIG informed about progress and developments related to its completion.

Recommendation 8: The Office of Executive Director should identify all eligibility determinations for access to classified information or holding a sensitive position adjudicated by the Securities and Exchange Commission since June 30, 2008, and, upon receipt of authority from the Director of National Intelligence (DNI), conduct a quality control assessment to ensure that the determinations were conducted in accordance with the uniform policies and procedures developed by the DNI.

OED Response: OED concurs with this recommendation and will conduct a quality review of eligibility determinations made by the SEC after June 30, 2008. These determinations were made consistent with E.O. 12968, and based upon the December 2005, *Revised Adjudicative Guidelines for Determining Eligibility for Access to Classified Information.* With only slight modifications in one area, these same guidelines have been adopted by the DNI in their *Personnel Security Adjudicative Guidelines for Determining Eligibility for Access to Sensitive Compartmented Information (SCI) and Other Controlled Access Program Information (IC Directive No. 704.2, effective October 2, 2008).* Based on the similarity between the current DNI adjudicative guidelines and the 2005 guidelines used by the OED to adjudicate the post June 30, 2008 cases, it is our belief that upon review these determinations will meet the current DNI adjudicative standards.

Thank you for your focus on this important area of agency operations, and for allowing us the opportunity to respond. If you have any questions regarding our response, please contact Carl Schilling at (202) 551-4358.

MEMORANDUM

March 24, 2011

TO: H. David Kotz
Inspector General

FROM: Sharon Sheehan
Associate Executive Director
Office of Administrative Services

SUBJECT: OAS Management Response to Draft Report No. 481, *Implementation of and Compliance with Homeland Security Presidential Directive 12*

This memorandum is in response to the Office of Inspector General's Draft Report No. 481, *Implementation of and Compliance with Homeland Security Presidential Directive 12*. Thank you for the opportunity to review and respond to this report. We concur with the nine recommendations addressed to OAS in the report and have begun taking appropriate steps to implement them.

Recommendation 3:

OAS concurs. OAS Security Branch will maintain a list of all contractors who are employed within the Commission, and develop policies and procedures for ensuring the list remains current.

Recommendation 4:

OAS concurs. In the policy or procedures guide, OAS will establish the frequency and method of transmittal of the consolidated list of contractor personnel employed within the Commission to the OHR Personnel Security Branch.

Recommendation 10:

OAS concurs. OAS will discontinue making eligibility determinations for persons requiring temporary access to the SEC and instead turn over the responsibility to the OHR Personnel Security Branch.

Recommendation 11:

OAS concurs. OAS Security Branch will turn over all documentation in its possession relating to the risk assessments conducted including lists of persons who have either been denied or granted access to SEC space and copies of all fingerprint records.

Recommendation 13:

OAS concurs. OAS Security Branch will provide guidance to Regional Office (RO) staff on the requirement to enroll personal identity verification (PIV) credentials into the RO physical access control systems. Guidance will also designate the PIV credential be the primary badge for physical access to SEC facilities.

Recommendation 17:

OAS concurs. OAS Security Branch will update the existing *Identification Cards, Press Passes and Proximity Access Control Cards* policy and post a revised access policy on the SEC intranet site.

Recommendation 18:

OAS concurs. OAS Security Branch will develop and implement a plan to systematically revoke all SEC-issued badges for all employees and contractors who have been issued HSPD-12 credentials. OAS will implement the plan within six months of the date of the final OIG report.

Recommendation 24:

OAS concurs. OAS Security Branch discussed this recommendation with OIT. OIT has confirmed that they will retain visitor control logs as specified in the National Archives and Records Administration's General Records Schedule.

Recommendation 25:

OAS concurs. OAS Security Branch will perform regular reviews of visitor logs to ensure visitors are not circumventing the HSPD-12 requirements.

MEMORANDUM

TO: H. David Kotz, Inspector General, Office of Inspector General

FROM: Thomas A. Bayer, Director, Office of Information Technology

RE: Office of Information Technology's Response to the Office of Inspector General's Report, *Implementation of and Compliance with Homeland Security Presidential Directive 12, Report No. 481*

DATE: March 25, 2011

This memorandum is in response to the Office of Inspector General's (OIG) Draft Report No. 481 entitled, Implementation of and Compliance with Homeland Security Presidential Directive 12. Thank you for the opportunity to review and respond to this report.

OIG Recommendations:

The draft report had three recommendations for the Office of Information Technology (OIT):

Recommendation 21: *The Office of Information Technology should immediately conduct an audit of its inventory to identify and track all keyboards and laptops that contain card readers.*

OIT concurs with this recommendation and is presently conducting an audit of its assets to identify all laptops and desktops that do not have HSPD-12 complaint keyboards/card readers. This effort will be complete within the next 30 days.

Recommendation 22: *The Office of Information Technology should promptly deploy appropriate technology (e.g., laptops with internal card readers, keyboards with card readers, or external card readers) to employees and contractors who do not have card readers.*

OIT concurs with this recommendation and upon completion of the asset audit to identify all laptops and desktops that do not have HSPD-12 complaint keyboards/card readers, OIT will deploy complaint devices to all SEC staff and contractors. This effort will be complete within the next 90 days.

Recommendation 23: *The Office of Information Technology should eliminate one-full time registrar and split the time of the other full-time registrar between the Operations Center and Headquarters locations.*

OIT concurs with this recommendation and will eliminate one full-time registrar after the ISS contract transition at the Operations Center. This effort will be complete within the next 120 days as the registrar contract expires.

OIG Response to Management's Comments

We are pleased that OAS, OED, OHR, and OIT have concurred with all of the report's 25 recommendations. We are also encouraged that these offices have indicated that they have already taken steps to implement the recommendations and have also, in several cases, provided timelines for when additional steps will be taken.

The OIG audit found deficiencies in nearly every aspect of the SEC's HSPD-12 program, as well as significant concerns about the SEC's authority to determine eligibility for access to classified information and the current process for granting temporary access to SEC facilities. Swift implementation of all of the report's recommendations is critical to ensuring that the SEC becomes compliant with the HSPD-12 directive.

Audit Requests and Ideas

The Office of Inspector General welcomes your input. If you would like to request an audit in the future or have an audit idea, please contact us at:

U.S. Securities and Exchange Commission
Office of Inspector General
Attn: Assistant Inspector General, Audits (Audit Request/Idea)
100 F Street, N.E.
Washington D.C. 20549-2736

Tel. #: 202-551-6061
Fax #: 202-772-9265
Email: oig@sec.gov

Hotline

To report fraud, waste, abuse, and mismanagement at SEC, contact the Office of Inspector General at:

Phone: 877.442.0854

Web-Based Hotline Complaint Form:
www.reportlineweb.com/sec_oig