August 1, 2006

MEMORANDUM TO: Luis A. Reyes
Executive Director for Operations

FROM: Stephen D. Dingbaum**/RA/**
Assistant Inspector General for Audits

SUBJECT: AUDIT OF NRC'S IMPLEMENTATION OF HOMELAND SECURITY PRESIDENTIAL DIRECTIVE-12 (HSPD-12) (OIG-06-A-20)

This report presents the results of the subject audit. Agency comments provided at the exit conference on July 10, 2006, have been incorporated, as appropriate, into this report. The agency did not provide formal comments.

Please provide information on actions taken or planned on each of the recommendations within 30 days of the date of this memorandum. Actions taken or planned are subject to OIG follow up as stated in Management Directive 6.1.

We appreciate the courtesies and cooperation extended to us by members of your staff during the audit. If you have any questions or comments about our report, please contact me at 301-415-5915, or Beth Serepca at 415-5911.

Attachment: As stated

Electronic Distribution

John T. Larkins, Executive Director, Advisory Committee on Reactor Safeguards/Advisory Committee on Nuclear Waste
G. Paul Bollwerk, III, Chief Administrative Judge, Atomic Safety and Licensing Board Panel
Karen D. Cyr, General Counsel
John F. Cordes, Jr., Director, Office of Commission Appellate Adjudication
Jesse L. Funches, Chief Financial Officer
Janice Dunn Lee, Director, Office of International Programs
Rebecca L. Schmidt, Director, Office of Congressional Affairs
Eliot B. Brenner, Director, Office of Public Affairs
Annette Vietti-Cook, Secretary of the Commission
William F. Kane, Deputy Executive Director for Reactor and Preparedness Programs, OEDO
Martin J. Virgilio, Deputy Executive Director for Materials, Research, State and Compliance Programs, OEDO
Jacqueline E. Silber, Deputy Executive Director for Information Services and Administration, and Chief Information Officer, OEDO
William M. Dean, Assistant for Operations, OEDO
Timothy F. Hagan, Director, Office of Administration
Michael R. Johnson, Director, Office of Enforcement
Guy P. Caputo, Director, Office of Investigations
Edward T. Baker, Director, Office of Information Services
James F. McDermott, Director, Office of Human Resources
Corenthis B. Kelley, Director, Office of Small Business and Civil Rights
Jack R. Strosnider, Director, Office of Nuclear Material Safety and Safeguards
James E. Dyer, Director, Office of Nuclear Reactor Regulation
Brian W. Sheron, Director, Office of Nuclear Regulatory Research
Janet R. Schlueter, Director, Office of State and Tribal Programs
Roy P. Zimmerman, Director, Office of Nuclear Security and Incident Response
Samuel J. Collins, Regional Administrator, Region I
William D. Travers, Regional Administrator, Region II
James L. Caldwell, Regional Administrator, Region III
Bruce S. Mallett, Regional Administrator, Region IV

AUDIT REPORT

Audit of NRC's Implementation of
Homeland Security Presidential
Directive-12 (HSPD-12)

OIG-06-A-20 August 1, 2006

EXECUTIVE SUMMARY

BACKGROUND

President Bush issued Homeland Security Presidential Directive-12 (HSPD-12) on August 27, 2004, to address wide variations in the quality and security of forms of identification used to gain access to Federal facilities. This directive ordered the establishment of a mandatory Governmentwide standard for secure and reliable forms of identification to be issued by the Government to its contractors and employees.

In February 2005, the National Institute of Standards and Technology (NIST) issued Federal Information Processing Standards Publication 201 (FIPS 201), "Personal Identity Verification (PIV) of Federal Employees and Contractors." This document specifies the requirements for a common identification standard for Federal employees and contractors. In March 2006, NIST issued a revision to FIPS 201. The revised document has the same title as FIPS 201, and is identified as FIPS 201-1. Differences between the two versions are irrelevant to the findings in this report.

FIPS 201-1 consists of two parts. The first, referred to as PIV-I, sets out uniform requirements for identity proofing (i.e., verifying the identity of individuals applying for official agency badges) as well as issuing badges, maintaining related information, and protecting the privacy of applicants. The second part, known as PIV-II, provides detailed specifications that will support technical interoperability[1] among Government department and agency personal identity verification systems.

PURPOSE

The objective of this audit was to determine whether the Nuclear Regulatory Commission (NRC) is positioned to meet HSPD-12 requirements.

RESULTS IN BRIEF

NRC implemented a PIV-I process in accordance with the Office of Management and Budget's (OMB) deadline and is considering options for PIV-II implementation. However, improvements are

[1] Interoperability is the ability of two or more systems or components to exchange information and to use the information exchanged.

needed to (1) assure consistent fulfillment of PIV-I requirements and (2) strengthen the HSPD-12 working group. In addition to these two audit findings, this report conveys an observation concerning the agency's approach to PIV-II. This observation, which appears in Appendix C, addresses the need to document PIV-II alternatives to ensure the agency pursues a cost-effective solution.

PIV-I Process Is Not Always Followed

NRC implemented a PIV-I process within the timeframe required by OMB. However, staff do not always follow certain PIV-I requirements contained in NIST guidance or in NRC's accredited PIV-I implementation plan. Auditors identified examples where:

- The required background investigation was not completed prior to badge issuance.
- Required identity documents were not reviewed prior to badge issuance.
- Required paperwork was not on file.
- The separation-of-duty requirement was not achieved in headquarters because a single individual has the ability to issue a badge without cooperation from any other participant in the process.

These problems occurred because (1) there is no quality assurance measure to assure that required steps are met prior to badge issuance, (2) some personnel with roles in the process do not understand their responsibilities, and (3) the badge photograph process is not carried out in accordance with the accredited plan. As a result, NRC (1) lacks assurance that the PIV-I process is consistently followed and (2) does not achieve the HSPD-12 separation-of-duty requirement.

Strengthen the HSPD-12 Working Group

NRC's HSPD-12 working group lacks a charter, lacks certain expertise that will be useful to guide the implementation of PIV-II, and has limited executive level representation. NRC's HSPD-12 working group is not sufficiently formalized or representative because Security Branch officials did not recognize the need for such measures. The development of an appropriate and cost-effective PIV-II solution will be facilitated by the efforts of a more formalized working group.

RECOMMENDATIONS

This report makes six recommendations to assure PIV-I requirements are fulfilled and to strengthen the HSPD-12 working group.

AGENCY COMMENTS

During an exit conference held July 10, 2006, the agency generally agreed with the audit findings and recommendations and provided comments concerning the draft audit report. We modified the report as we determined appropriate in response to these comments. NRC reviewed these modifications and opted not to submit formal written comments to this final version of the report.

[Page intentionally left blank.]

TABLE OF CONTENTS

[Page intentionally left blank.]

ABBREVIATIONS AND ACRONYMS

FBI	Federal Bureau of Investigation
FIPS	Federal Information Processing Standards Publication
GAO	Government Accountability Office
HSPD-12	Homeland Security Presidential Directive-12
MD	Management Directive and Handbook
NRC	Nuclear Regulatory Commission
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PIV	Personal Identity Verification

[Page intentionally left blank.]

I. BACKGROUND

President Bush issued Homeland Security Presidential Directive-12 (HSPD-12) on August 27, 2004, to address wide variations in the quality and security of forms of identification used to gain access to Federal facilities. This directive ordered the establishment of a mandatory Governmentwide standard for secure and reliable forms of identification to be issued by the Government to its contractors and employees.

HSPD-12 assigned specific responsibilities and deadlines to different Government entities. It directed the Secretary of Commerce, within 6 months of the directive's issuance, to issue a standard for secure and reliable forms of identification that:

- Establishes a reliable process for verifying an individual's identity.
- Is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation.
- Can be verified electronically in an expeditious manner.
- Is distributed only by an authorized provider whose reliability has been established in an official accreditation process.

It directed Government departments and agencies to require Federal employees and contractors to use identification that meets the standard to gain physical and logical access to Federal facilities and information systems.[2] This was to be accomplished within 8 months of the standard's issuance and to the maximum extent practicable. It directed the Office of Management and Budget (OMB) to ensure compliance with the directive and standard. (See Table 1 for a list of dates related to HSPD-12.)

[2] Physical access refers to the physical access to the computing systems, facilities, and paper records. Logical access refers to user based authenticated access to computers, application systems, and the data that is processed.

Table 1. HSPD-12 Dates	
August 2004	President issues HSPD-12
February 2005	NIST issues FIPS 201
August 2005	OMB issues HSPD-12 implementation guidance memo
October 2005	Deadline for agency compliance with PIV-I
March 2006	NIST issues FIPS 201-1
October 2006	Deadline for agencies to begin issuing HSPD-12 badges
October 2007	Deadline for agencies to finish issuing HSPD-12 badges

FIPS 201 and 201-1

In February 2005, the National Institute of Standards and Technology (NIST) (part of the Department of Commerce) issued Federal Information Processing Standards Publication 201 (FIPS 201), "Personal Identity Verification (PIV) of Federal Employees and Contractors." This document specifies the requirements for a common identification standard for Federal employees and contractors. In March 2006, NIST issued a revision to FIPS 201. The revised document has the same title as FIPS 201, and is identified as FIPS 201-1. Differences between the two versions are irrelevant to the findings in this report.

FIPS 201-1 consists of two parts. The first, referred to as PIV-I, sets out uniform requirements for identity proofing (i.e., verifying the identity of individuals applying for official agency badges) as well as issuing badges, maintaining related information, and protecting the privacy of applicants. Table 2 lists some of the main PIV-I requirements.

Table 2. Selected PIV-I Requirements
❖ Successfully completed background investigation
❖ Two original identification documents
❖ Applicant appears in person prior to badge issuance
❖ Verification, at badge issuance, that the recipient is the same as the intended recipient
❖ A single individual cannot issue a badge without the cooperation of another authorized person
❖ Full disclosure to badge recipients of intended uses of the badge and related privacy implications

The second part, known as PIV-II, provides detailed specifications that will support technical interoperability among Government department and agency personal identity verification systems. This interoperability is based on the use of interoperable smart cards, which are plastic, credit card sized devices that use integrated circuit chips to store and process data. Smart cards offer the potential to enhance security by improving the process of authenticating the identity of people accessing Federal buildings and computer systems, especially when used in combination with other technologies, such as biometrics.[3]

[3] A biometric measures a person's unique physical characteristics (e.g., fingerprints, hand geometry) or behavioral characteristics (e.g., voice patterns, written signatures) and can be used to recognize the identity, or verify the claimed identity, of an individual.

PIV-II Minimum Requirements

Although FIPS 201-1 describes the minimum requirements to allow interoperability of the PIV smart cards for physical and logical access, it does not prescribe the extent to which agencies should use the cards for such purposes. According to FIPS 201-1, it is up to Federal departments and agencies to determine the level of security and authentication mechanisms appropriate for their applications. As explained by a NIST official, the FIPS standard and its associated guidelines specify what is to be on the card in order to support a range of physical and logical access control mechanisms, but do not specify what mechanisms should be employed.

Table 3 lists some of the minimum requirements for a PIV-II compliant system.[4] Also see Appendix A for an architectural diagram of components that may be included in a PIV-II system.

[4] These requirements appeared on an OMB HSPD-12 reporting template that Federal agencies were required to complete and submit to OMB for review and approval. Federal agencies were asked to provide a status and planned completion date for each of these requirements.

Table 3. Selected PIV-II Requirements
❖ Badges are issued through systems and providers whose reliability has been established by the agency through a self-accreditation process.
❖ All agency badges are issued with FIPS 201 visible external security features.
❖ All agency badges are issued with FIPS 201 electronic security features.
❖ Agency employees and contractors routinely use these electronic security features to gain access to facilities and/or systems (or to authenticate identity).
❖ Badges contain a biometric and can be electronically authenticated to the holder using a biometric match.
❖ Badges have the capability to be electronically verified to determine the employee/contractor is in good standing (i.e., badge has not been revoked).

OMB Guidance

In August 2005, OMB issued HSPD-12 implementation guidance for Federal departments and agencies. This guidance directed agencies to implement PIV-I requirements by October 27, 2005. It also directed agencies to begin issuing HSPD-12 badges that meet PIV-II requirements by October 27, 2006, to employees and contractors needing routine access to Federal facilities or information systems for more than 6 months. OMB mandated that departments and agencies use only products and services that are approved as compliant with the FIPS standard and are included on an approved products list.

Current Status of HSPD-12 Implementation

In February 2006, the Government Accountability Office (GAO) reported that the Federal Government faces significant challenges in implementing the FIPS 201 standard, including:

- Testing and acquiring compliant commercial products, such as smart cards and card readers within OMB-mandated deadlines.
- Reconciling divergent implementation specifications.
- Incomplete guidance regarding the applicability of the standard to facilities, people, and information systems.
- Planning and budgeting with uncertain knowledge and the potential for substantial cost increases.

The report also assessed the progress of six agencies – the Departments of Defense, the Interior, Homeland Security, Housing and Urban Development, and Labor, and the National Aeronautics and Space Administration – in implementing PIV-I and PIV-II. GAO found that the six agencies had focused primarily on PIV-I and had begun to address PIV-II, but had not developed specific designs for card systems that met FIPS 201 interoperability requirements. Five of the six agencies reported that they had made little progress toward implementing PIV-II due largely to the absence of FIPS 201 compliant products.[5]

NRC's Progress

The Nuclear Regulatory Commission (NRC) implemented a PIV-I process on October 27, 2005, in compliance with OMB's deadline. The agency's PIV-I process establishes five PIV-I roles: (1) applicant, (2) PIV sponsor, (3) PIV registrar, (4) I-9 document certification authority, and (5) PIV issuer. Table 4 provides information on each of these roles.

Implementation of the PIV-I process did not require major adjustments to NRC's existing personnel security program, which already required all employees and contractors to undergo background investigations prior to being permitted unescorted access within NRC facilities. The main changes are that (1) employees and contractors now must present two specific forms of

[5] GAO-06-178, *Electronic Government – Agencies Face Challenges in Implementing New Federal Employee Identification Standard*, was published in February 2006, prior to the issuance of FIPS 201-1.

original identification documents prior to being issued a badge and (2) some contractors undergo a higher level background investigation than previously was required. Also, due to HSPD-12's separation-of-duty requirement (i.e., that no single individual may issue a badge without the cooperation of another authorized individual), there are more people involved in the badging process than before.

Table 4. HSPD 12 Roles and Descriptions

HSPD-12 Role	Description
Applicant	The contractor or employee to whom a badge is issued.
PIV Sponsor (performed by the Office of Human Resources)	The individual who validates an applicant's requirement for a PIV badge and sponsors the applicant's request.
PIV Registrar (performed by designated staff in the headquarters Security Branch)	The individual or entity that performs the identity-proofing process for the applicant and ensures that the proper background checks have taken place with positive results. The PIV registrar has the final approval authority for issuance of a badge to an applicant.
I-9 Document Certification Authority (performed by designated staff in headquarters, the regional offices, and at resident inspector sites)	The individual who assists the PIV registrar by performing the identity-proofing process for the applicant.
PIV Issuer (performed by designated headquarters Security Branch staff and security guards, regional office, and resident inspector site staff)	The individual or entity that issues a badge to an applicant following the positive completion of all identity proofing, background checks, and related approvals.

The PIV-II process is expected to bring more visible changes to NRC's process. In October 2005, the Commission approved the NRC staff's plan for implementing PIV-II in a timeframe acceptable to OMB. According to NRC staff, implementing NRC's planned PIV-II approach, which exceeds PIV-II minimum requirements, would cost $10.2 million. Further, it would serve to enhance the agency's physical and personnel security capabilities. The plan includes:

- Perimeter access control devices at headquarters and regional entry points to read the HSPD-12 badge, verify its authenticity, and allow access.
- Logical access readers for all employee and contractor workstations in headquarters and regional offices.
- Fingerprint and photo capture stations in headquarters and regional offices.
- Badge encoders in headquarters and regional offices and badge printers in headquarters.
- Turnstiles for headquarters lobbies.
- A new automated system to support HSPD-12, personnel security, and physical security requirements.

As part of its implementation efforts, NRC established an NRC HSPD-12 working group composed of 13 individuals from the Offices of Administration and Information Services that meets periodically to discuss developments and concerns related to implementation of PIV-II at NRC.

II. PURPOSE

The objective of this audit was to determine whether NRC is positioned to meet HSPD-12 requirements. Appendix B contains information on the audit scope and methodology.

III. FINDINGS

NRC implemented a PIV-I process in accordance with OMB's deadline and is considering options for PIV-II implementation. However, improvements are needed to (1) assure consistent fulfillment of PIV-I requirements and (2) strengthen the HSPD-12 working group. In addition to these two audit findings, this report conveys an observation concerning the agency's approach to PIV-II. This observation, which appears in Appendix C, addresses the need to document PIV-II alternatives to ensure the agency pursues a cost-effective solution.

A. PIV-I Process Is Not Always Followed

NRC implemented a PIV-I process within the timeframe required by OMB. However, staff do not always follow certain PIV-I requirements contained in NIST guidance or in NRC's accredited PIV-I implementation plan. Auditors identified examples where:

- The required background investigation was not completed prior to badge issuance.
- Required identity documents were not reviewed prior to badge issuance.
- Required paperwork was not on file.
- The separation-of-duty requirement was not achieved in headquarters because a single individual has the ability to issue a badge without cooperation from any other participant in the process.

These problems occurred because (1) there is no quality assurance measure to assure that required steps are met prior to badge issuance, (2) some personnel with roles in the process do not understand their responsibilities, and (3) the badge photograph process is not carried out in accordance with the accredited plan. As a result, NRC (1) lacks assurance that the PIV-I process is consistently followed and (2) does not achieve the HSPD-12 separation-of-duty requirement.

NIST and NRC Requirements

FIPS 201-1 specifies the minimum requirements for a Federal personal identity verification system that meets HSPD-12's control and security objectives. According to FIPS 201-1, departments and agencies are to adopt and use a self-accredited process for verifying applicant identities and issuing and maintaining applicant badges. Departments and agencies are required to accredit their process by determining that it satisfies requirements, and the head of the entity is to approve the process in writing.

These requirements fall into three categories: (1) *identity proofing and registration requirements* used to verify the identity of the employee or contractor; (2) *badge issuance and maintenance requirements* pertaining to badge production and issuance to the employee or contractor; and (3) *privacy requirements* intended to protect the personal privacy of employees and contractors subject to HSPD-12 requirements. Requirements include the following:

- A minimum background investigation must be completed prior to badge issuance. FIPS 201-1 requires that the Federal Bureau of Investigation (FBI) National Criminal History Fingerprint Check, which is one component of the National Agency Check, be completed before badge issuance.

- The employee or contractor must provide two forms of original identity documents. These documents must come from the list of acceptable documents in Department of Homeland Security Form I-9, Employment Eligibility Verification. (See Table 5 for examples of acceptable I-9 documents.)

- PIV applicants must be fully informed as to the intended uses of the badge and the related privacy implications.

- The PIV identity proofing, registration, and issuance process must adhere to the separation-of-duty requirement to ensure that no single individual has the capability to issue a badge without the cooperation of another authorized person.

NRC's accredited PIV-I process describes an approach that meets FIPS 201-1 requirements, including those listed in the previous paragraph. The process establishes specific PIV-I roles. For example, *PIV registrars* in the Security Branch at headquarters are responsible for ensuring that the necessary background investigation is complete and reviewing the two original I-9 documents prior to badge issuance. In the regional offices and at

resident inspector sites, this role is assisted by *I-9 document certification authorities*, who review the two original I-9 documents and certify to the headquarters registrars that the documents are appropriate and authentic. *PIV issuers* in the regional offices, resident inspector sites, and headquarters issue badges to the employee or contractor after all prerequisites are met.

Table 5. Examples of I-9 Documents

- U.S. Passport, expired or unexpired
- Unexpired foreign passport
- Certificate of U.S. Citizenship
- Certificate of Naturalization
- Driver's license
- Federal, State, or local government identification card
- School ID card
- Voter's registration card
- U.S. Social Security card
- U.S. military card or draft record
- U.S. citizen identification card

NRC's Process Was Not Always Followed

NRC's PIV-I process was not consistently followed in that:

- The required background investigation was not always completed prior to badge issuance.

- Two forms of I-9 documents were not always reviewed prior to badge issuance.

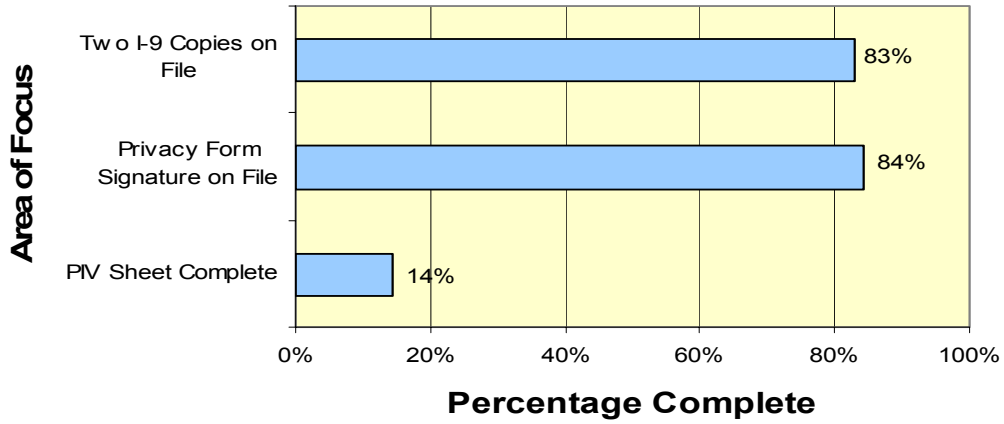
- The form indicating that the applicant was notified of privacy implications was not always on file.

- At headquarters, the separation-of-duty requirement was not met. The issuer, who takes the photographs for headquarters employees and contractors and issues badges to these individuals, has the ability to issue a badge without cooperation from any other participant in the process. In contrast, separation of duties occurs in the NRC regional offices because the badge photographs are taken in the regional offices and the badges are produced at headquarters.

Background Investigation

Auditors conducted a file review to assess how well the PIV-I process was followed for 72 employees and 4 contractors hired during the first 4 months that the process was implemented and identified two instances where the required background check was not complete prior to badge issuance. In one case, the FBI National Criminal History Fingerprint Check had not been returned and in the other case, the fingerprint check was returned, but not all components of the National Agency Check were complete. Both instances occurred during the period of time when both FIPS 201 and NRC's accredited PIV-I plan required the return of the National Agency Check.[6]

Figure 1. File Review Results
(based on 76 files reviewed)



I-9 Documentation

Two indicators suggested inconsistency with regard to the review of two I-9 documents for each applicant. First, auditors found three examples where contractors were required to present only one I-9 document for review prior to badge issuance. Second, auditors identified 10 employee files that did not contain copies of two I-9 documents. Of the 10 incomplete employee files, 8 contained no

[6] Prior to March 2006, under the original FIPS 201, the required investigation was the National Agency Check. Now, however, the revised FIPS 201-1 requires that only one component of the National Agency Check – the FBI National Criminal History Fingerprint Check – be completed before badge issuance. NRC issued revision 1 of its accredited PIV-I plan on March 24, 2006, after OIG identified cases where badges had been issued prior to the return of the fingerprint check. The revised document states that badges may be issued following return of the fingerprint check.

I-9 document copies at all. The three contractor examples provide actual cases where the process was not followed, whereas the absence of documents in the other files suggests other occasions where the process may not have been followed. While the absence of documents in the files does not prove definitively that the documents were not reviewed, it likewise does not prove that the documents were reviewed. To ensure consistency, copies of two I-9 documents should be included in each file. See Figure 1 on page 12 for information on the file review results.

Privacy Form

To verify that applicants are informed about the privacy issues relevant to the PIV-I process, applicants are asked to review a Privacy Act statement concerning the badge issuance process and to sign a form acknowledging their review of the statement. The Security Branch maintains some of these forms in individual personnel security folders and others in a binder used specifically to store these forms.

During the file review, auditors could not locate signed forms for 12 individuals in either location. Although the absence of these documents does not prove that applicants were not informed about the Privacy Act concerns, it does not provide assurance that the appropriate step occurred.

Separation of Duties

NRC's PIV-I process specifies that photographs for employees and contractors are to be taken by PIV registrars in headquarters and by the I-9 certification authorities in the regional offices and at resident inspector sites. However, this requirement is not fulfilled in headquarters, where the issuers, and not the registrars, take the photographs. Because it is the headquarters issuers who also produce the badges and issue them to headquarters employees, these individuals have the capability of creating and issuing badges without the input from any other individual with a role in the process.

Separation of duties does occur in the regional offices because while the badge photographs are taken in those locations, the badge production occurs at headquarters.

Process Adjustments Are Needed

These problems occurred because:

- There is no quality assurance measure to assure that required steps are met prior to badge issuance.
- Some with roles in the process do not understand their responsibilities.
- The badge photograph process is not carried out in accordance with the accredited plan.

Quality Assurance Measure Is Absent

NRC has issued badges to employees who did not complete the prerequisites to badge issuance because there is no quality assurance measure in the process to ensure all necessary steps are completed prior to issuance. No individual is assigned the task of reviewing all prerequisite steps prior to sending the signal to the badge creators that a badge is now warranted.

Currently, the notification to the headquarters issuers to produce and issue a badge is signaled by the transmittal of NRC Form 236, "Personnel Security Clearance Request and Notification," for employees and NRC Form 89, "Badge Request," for contractors. Both forms are used to provide information to the Security Branch as to what type of clearance or access is needed. Although each form is completed by a Security Branch official and forwarded to the issuers from the Security Branch, neither form provides information concerning the status of the PIV-I process (e.g., background investigation complete, two I-9 documents provided) to indicate that all necessary prerequisites are complete.

The Security Branch developed and uses a Personal Identity Verification Sheet to track the PIV-I process. This form, which is maintained in the personnel security files, is often incomplete, and therefore not a useful indicator of whether prerequisite steps were accomplished. Of the 76 verification sheets reviewed during the audit, only 11 were completely filled out. If the Security Branch were to require completion of the form, this would be a useful tool to review as a quality control measure prior to badge issuance.

Lack of Understanding of Responsibilities

Another reason staff do not consistently follow the PIV-I process is that some individuals with roles in the process do not fully understand their responsibilities. In headquarters, five individuals with the registrar role expressed or demonstrated misunderstandings about such aspects of the process as:

- How contractors are handled.
- The type of background investigation needed prior to badge issuance.
- Whether unescorted access is permitted prior to provision of two I-9 documents.
- Whether issuers need to review copies of two I-9 documents prior to badge issuance.

Regional staff with HSPD-12 roles were generally less familiar with their responsibilities than headquarters staff due to the small number of regional staff and contractors hired for those locations since October 27, 2005 (the date NRC implemented its PIV-I process). Three of seven regional employees contacted by the Office of the Inspector General (OIG) had not received formal training on their role and two had not received any written guidance. Moreover, one individual incorrectly thought that the HSPD-12 process for regional contractors would be handled entirely by headquarters.

Process for Badge Photographs Does Not Follow Plan

Separation of duties is not achieved in headquarters because staff are not following the process described in the accredited PIV-I plan which assigns badge photographs to the registrar. Allowing issuers to take the photographs and produce and issue the badges gives them the ability to single-handedly produce badges without input from anyone else in the process. A Security Branch official said they have prepared an area within their office space to allow headquarters registrars to take the photos, but have yet to implement this process.

During the audit exit conference, an NRC official said the Security Branch registrars had begun taking the badge photographs and that this task was no longer being performed by the headquarters issuers.

No Assurance That Process Is Followed

NRC lacks assurance that its PIV-I process is consistently followed and does not achieve the HSPD-12 separation-of-duty requirement. Implementing measures to assure the process is followed and imposing the separation-of-duty requirement will assist the Security Branch Chief in his ongoing HSPD-12 responsibility to ensure that badges are produced and issued in accordance with requirements.

Recommendations

OIG recommends that the Executive Director for Operations:

1. Assign an individual or individuals to ensure that all PIV-I requirements are met prior to initiating a request to the issuer to produce and issue a badge.

2. Require completion of the Personal Identity Verification Sheet to track the PIV-I process and use this form to initiate the badge request.

3. Provide NRC-specific HSPD-12 training to all individuals with roles in the process to ensure they understand their responsibilities and the process overall. This training should include the provision of written guidance, such as checklists of responsibilities, to all individuals with roles in the process.

4. Implement rules for separation-of-duty with regard to badge photographs.

B. HSPD-12 Working Group Has Several Shortcomings

NRC's HSPD-12 working group lacks a charter, lacks certain expertise that will be useful to guide the implementation of PIV-II, and has limited executive level representation. NRC's HSPD-12 working group is not sufficiently formalized or representative because Security Branch officials did not recognize the need for such measures. The development of an appropriate and cost-effective PIV-II solution will be facilitated by the efforts of a more formalized working group.

Working Groups

Important agency projects benefit from formalized working groups. Membership should include all NRC offices whose business processes will be affected by project implementation. Working groups can be critical to project development and implementation if their mission and member roles and responsibilities are clear to all parties. The importance of formalizing working groups is noted in two NRC Management Directives and Handbooks (MD) and by existing practice.

MDs 5.3 and 6.3

MD 5.3, "NRC/Agreement State Working Groups," describes the steps and process the staff should follow in establishing and implementing NRC/Agreement State working groups. MD 6.3, "The Rulemaking Process," specifies guidance for working groups tasked with supporting the rulemaking process.

Although these MDs focus on specific working groups, the guidance is applicable to other projects. For example, MD 5.3 describes the information that should be included in a working group's charter, such as purpose, membership, schedule, and expected product/outcome of the working group. MD 5.3 states that the lead organization usually assumes lead responsibility for the working group, including establishing the purpose of the working group, requesting participation, drafting a charter, identifying members, and tracking progress. This guidance also explains that working group members should be active in recommending improvements and should understand how their contributions are used in the process and products.

MD 6.3 specifies guidance for working groups tasked with meeting agency rulemaking objectives. Membership should include (1) a task leader from the lead office, (2) members from within the lead

office that have program responsibilities related to the rulemaking, (3) a member from the Office of the General Counsel to provide legal advice and support, and (4) staff from other offices, as appropriate.

Working Group Examples

The role of working groups has been defined in various internal and external efforts. Current NRC working groups include the Management Directives Working Group, the High-Level Waste - Information Support Program Executive Steering Committee, and Rulemaking Working Groups. Working groups such as these have established charters and consist of executive, management, and staff representatives from a range of NRC offices. In addition, two agencies interviewed during the course of this audit have established working groups to promote HSPD-12 implementation. Appendix D contains a sample of an HDPD-12 working group charter provided by another Federal agency.

HSPD-12 Not Sufficiently Formalized

The project to implement HSPD-12 is not benefiting from the input of a structured, formalized working group. Specifically, NRC's HSPD-12 working group:

- Has not established a charter.
- Lacks some expertise that will be needed to guide the implementation of PIV-II.
- Has limited executive level management representation.

Charter Not Established

NRC's HSPD-12 working group has not established a charter defining its purpose, mission, roles and responsibilities, and products. In addition, there are no formal records documenting meeting agenda or minutes or status of unresolved issues.

Lacks Certain Expertise

The current HSPD-12 working group lacks certain expertise that will be useful to guide the implementation of PIV-II and does not represent all NRC offices whose business processes will be affected when PIV-II is being implemented.

The current HSPD-12 working group does not include representation from offices outside the Office of Information Services and the Office of Administration, and also does not include some expertise from within these offices needed to facilitate a PIV-II solution. For example, there is no representative from the Division of Contracts to help with acquisition strategy, no representative from the Office of the General Counsel to provide legal advice concerning a PIV-II solution, and no representative from the Office of the Chief Financial Officer to assist with financial issues. In addition, the Office of Information Services staff person who was instrumental in costing out and encouraging the PIV-II planning approach is not a working group member.

Limited Executive Level Management Involvement

NRC's HSPD-12 working group has limited executive level management representation. The HSPD-12 working group is composed of 12 NRC employees and 1 contractor. Although the majority of the participants are grade 13 or above, only one member is a senior level executive and this individual, from the Office of Information Services, rarely attends the working group meetings.

Need For Structure Not Recognized

The absence of an HSPD-12 working group charter, limited executive level management, or diverse intra-agency representation within the HSPD-12 working group occurred because Security Branch staff did not recognize the need for input from such a group during the initial phase of HSPD-12 implementation. The Security Branch developed the PIV-I plan internally and involved other offices only for the PIV-I accreditation process. However, for PIV-II development and implementation, the input from a formalized working group will be increasingly important to complete these more technical tasks that will affect the business processes of all NRC offices.

Facilitation of Cost-Effective Solution

The development of an appropriate and cost-effective PIV-II solution will be facilitated by the efforts of a more formalized working group.

Recommendations

OIG recommends that the Executive Director for Operations:

5. Expand the HSPD-12 working group by including representation from all offices needed to facilitate a cost-effective PIV-II solution.

6. Formalize the HSPD-12 working group by developing a charter that defines the membership and expectations.

IV. AGENCY COMMENTS

During an exit conference held July 10, 2006, the agency generally agreed with the audit findings and recommendations and provided comments concerning the draft audit report. We modified the report as we determined appropriate in response to these comments. NRC reviewed these modifications and opted not to submit formal written comments to this final version of the report.

V. CONSOLIDATED LIST OF RECOMMENDATIONS

OIG recommends that the Executive Director for Operations:

1. Assign an individual or individuals to ensure that all PIV-I requirements are met prior to initiating a request to the issuer to produce and issue a badge.

2. Require completion of the Personal Identity Verification Sheet to track the PIV-I process and use this form to initiate the badge request.

3. Provide NRC-specific HSPD-12 training to all individuals with roles in the process to ensure they understand their responsibilities and the process overall. This training should include the provision of written guidance, such as checklists of responsibilities, to all individuals with roles in the process.

4. Implement rules for separation-of-duty with regard to badge photographs.

5. Expand the HSPD-12 working group by including representation from all offices needed to facilitate a cost-effective PIV-II solution.

6. Formalize the HSPD-12 working group by developing a charter that defines the membership and expectations.

APPENDIX A

PIV-II ARCHITECTURE DIAGRAM

The Architecture Diagram (page 24) provides a high-level overview of the components required to implement a FIPS 201 compliant system. The system components are as follows:

- The Identity Management System (IDMS) is the central component that interacts either directly or indirectly with all other components of the PIV-II Architecture.

- Registration stations are used to identity proof applicants and capture their biometrics for use in conducting background investigations and printing information on the PIV card.

- The public key infrastructure (PKI) component of the system will issue digital certificates, manage the keys associated with those certificates, and maintain up to date information on certificate status.

- The card management system (CMS) is used to manage card lifecycle activities. The CMS interfaces with the IDMS as well as the certificate authority, card printing station, and the PIV card itself. The CMS will be used to manage the issuance and printing of a PIV card and the public key infrastructure certificate associated with that card.

- The card printing system (CPS) will manage the printing and distribution of the actual PIV cards. Card printing and distribution will interface directly with the CMS and the applicant and indirectly with PKI, and IDMS.

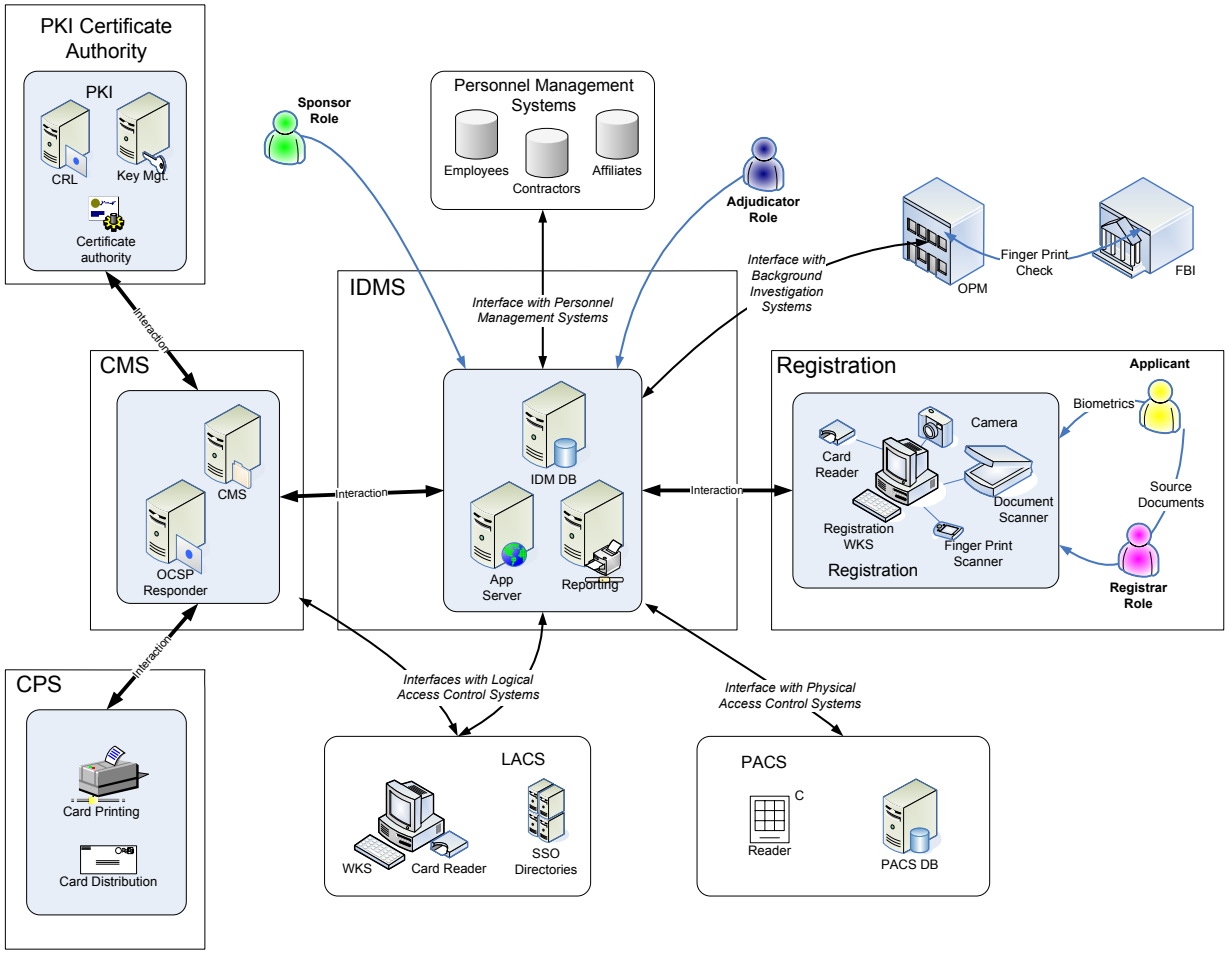
- Employee Data serves as the authoritative data source for providing information to the IDMS. All applicant information must first be present in the Employee data system before it is available to the IDMS; no applicant information will be entered directly into the IDMS.

- Office of Personnel Management (OPM) will conduct all applicant background investigations and forward results to the appropriate agency for adjudication. The FBI will be responsible for conducting fingerprint checks against its fingerprint database as a component of all background investigations.

- Logical Access Control Systems (LACS) will interface with PIV cards to provide cardholders access to federally controlled networks and information systems.

- Physical Access Control Systems (PACS) will interface with PIV cards to provide cardholders access to federally controlled facilities.

HSPD-12 Core Components



Appendix B

SCOPE AND METHODOLOGY

Auditors evaluated whether NRC is positioned to meet HSPD-12 requirements.

The OIG audit team reviewed relevant criteria, including HSPD-12, OMB guidance concerning HSPD-12, and NIST guidance, including FIPS 201 and FIPS 201-1. The audit team also reviewed NRC's documentation of its accredited PIV-I process as well as correspondence between NRC and OMB concerning HSPD-12 funding.

Auditors interviewed staff from the Office of Information Services and the Office of Administration concerning HSPD-12 implementation. Auditors interviewed regional and headquarters staff with roles in NRC's HSPD-12 process to assess their understanding of the process. Auditors also interviewed representatives from the Office of Personnel Management and the National Archives and Records Administration to learn about their implementation of HSPD-12 and communicated with staff from OMB and NIST concerning HSPD-12 requirements.

Auditors compared NRC's accredited HSPD-12 process with FIPS 201-1 and with OMB requirements, and observed aspects of the process as implemented in headquarters to assess whether the NRC's process and procedures met HSPD-12 objectives. Auditors also reviewed 76 personnel security files for both NRC employees and contractors with Entry on Duty dates of October 27, 2005, through February 28, 2006.

This work was conducted from December 2005 through March 2006, in accordance with generally accepted Government auditing standards and included a review of management controls related to audit objectives. The work was conducted by Beth Serepca, Team Leader; Judy Gordon, Audit Manager; Vicki Foster, Senior Management Analyst; and Erica Horn, Auditor.

[Page intentionally left blank.]

Appendix C

AUDIT OBSERVATION CONCERNING NRC'S PIV-II APPROACH

NRC, like other Federal agencies, is challenged to meet OMB implementation deadlines because approved products are not yet available, uncertainty persists over basic requirements, and additional money was not provided to implement HSPD-12. Given the lack of products or additional resources, and a Governmentwide initiative to look for cost-effective ways to implement HSPD-12, NRC has an opportunity to consider less expensive options than the agency initially envisioned in its $10.2 million PIV-II budget estimate. That budget estimate reflects a PIV-II plan that goes beyond minimum PIV-II requirements and does not take advantage of opportunities to share resources with other agencies.

While agency officials explained that they are continually considering alternative approaches, and have shifted their plan with regard to an OMB deadline, they had not documented such alternatives until recently. During the audit exit conference, NRC managers informed OIG that the $10.2-million approach was no longer the only documented approach under consideration. They explained that in May 2006 (after fieldwork on this audit was complete), the Office of Administration presented estimated costs for alternative approaches, including the use of a shared service provider, to NRC's Program Review Committee for consideration in the agency's budget process.

OMB Deadlines

OMB established October 27, 2006, as the date that Federal agencies are to begin issuing PIV-II badges and October 27, 2007, as the point at which compliant badges are to have been issued to all employees and contractors. At NRC's request, OMB allowed NRC a more generous timetable for compliance. Under the NRC plan that OMB approved, NRC proposed to begin issuing badges on September 28, 2007, and finish issuance by February 28, 2008.

NRC's Schedule

Because no additional funding was provided to NRC for HSPD-12 implementation, and because approved HSPD-12 products were not available earlier this year as anticipated,[7] NRC does not intend to meet the OMB-approved dates. Instead, the agency intends to

[7] As of the drafting of this report, approved, HSPD-12 compliant products were still unavailable.

revert to a prior timeline that OMB disapproved. Under that plan, the agency proposed to begin issuing compliant badges in November 2008. However, a Security Branch official said that NRC would issue a single badge in October 2006 to fulfill OMB's requirement to begin issuing PIV-II compliant cards at that time.

NRC's PIV-II Plans

While agency officials explained that they are continually considering alternative approaches to a $10.2 million PIV-II plan that they developed, they have not, until recently, documented these alternatives.

The $10.2 million plan, which is documented and which served as the basis for the timeline approved by OMB, reflects an approach that may be warranted to strengthen security at NRC. This plan exceeds minimum HSPD-12 requirements by including logical access readers on every employee's workstation, lobby turnstiles, fingerprint authenticators, a new badge access system, a new personnel security system, and in-house badge manufacturing capabilities. (See the Background section of this report for information on minimum requirements.)

Security Branch officials' perspectives toward the documented approach have shifted over time. At the start of this audit, a Security Branch official explained that this solution was desirable because it would allow employees to have one badge access card instead of two (e.g., one for NRC access and one that is HSPD-12 compliant) and would eliminate the need to "sneakernet"[8] data from the personnel security database to the badge access database. The official also said that in-house badging capability was desirable because it would prevent inconveniencing NRC staff whom, under a shared resources approach (e.g., relying on another agency's badge manufacturing capabilities), would have to commute to an offsite location to obtain initial and replacement badges.

More recently, however, a Security Branch official described the $10.2 plan as an outside guess based on the "worst case" in that it allows for all possibilities and the uncertainties in terms of product availability and cost. This official explained that the Security Branch is considering alternative approaches, including the sharing of resources with other agencies. Although NRC officials are contemplating alternatives to the $10.2 million approach

[8] Sneakernet is a term used to describe the practice of sharing data by copying files to floppy diskettes, and walking them to another part of the office to load them onto another computer. It is a way of sharing data and files in the absence of a local area network.

documented to support the plan and schedule approved by OMB, the agency has only recently begun to document these alternatives.

By continuing to document the alternative approaches to PIV-II that are currently under consideration, and the timelines and costs for implementing these approaches, NRC will be better positioned to pursue a cost-effective course of action.

[Page intentionally left blank.]

Appendix D

SAMPLE CHARTER

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE-12 PERSONAL IDENTITY VERIFICATION WORKING GROUP

The Personal Identity Verification (PIV) Working Group is a stakeholders working group supported by voluntary participation from the key NRC organizations impacted by PIV implementation.

1. Mission.

The Personal Identity Verification (PIV) Working Group is designed to support collaborative implementation of Homeland Security Presidential Directive-12 (HSPD-12), ensuring that the agencywide personal identity program meets the control and security objectives of HSPD-12, to include identity proofing, registration and issuance.

2. Scope.

The PIV Working Group supports the agency's PIV implementation efforts by:

a. Serving in an advisory capacity.

b. Facilitating integration among stakeholder departments to promote proper selection and use of the best available equipment and procedures to optimize safety, interoperability, and efficiency.

c. Identifying technical, physical security, and facilities requirements for PIV implementation.

d. Providing a catalyst for recommendations to the Interagency Advisory Board (IAB) on interoperability solutions between Federal agencies.

e. Establishing policy and procedures for the operation and maintenance of the agency's PIV program.

SAMPLE CHARTER

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE-12
PERSONAL IDENTITY VERIFICATION WORKING GROUP

3. Organizational Structure and Responsibilities.

   a. Chairman – The PIV Working Group Chairman is _____ and Co-Chairs are _____ ; all of the Division_____. The Chairman is selected by default as part of the position description of the PIV Physical Security Specialist. The Chairman's term starts at EOD and ends when this individual transitions out of the position.

The Chairman administers, organizes, and facilitates the actions of the PIV Working Group.

The Chairman provides recommendations to the Executive Stakeholders Committee through the _____.

   b. Working Group Membership

SubGroups/ Co-Chairs

SubGroups– The PIV Working Group has five SubGroups which consist of subject matter experts:

1. Physical Security
2. Information Systems
3. Contracting and Facilities
4. Human Capital
5. Executive Stakeholders

SubGroups will send Primary and /or Backup representatives to act as Co-chairs.

The duties of SubGroup/Committee Co-Chairs are to:

   a. Direct the efforts within their sub-groups to accomplish the scope of PIV working group activities, to support overall PIV implementation and maintenance.

   b. Provide liaison with the PIV Working Group Chairman.

   c. Provide meeting minutes, status of ongoing projects, and written reports of recommendations and requirements from the SubGroup.

SAMPLE CHARTER

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE-12
PERSONAL IDENTITY VERIFICATION WORKING GROUP

d. Chairs to review membership participation and to ensure SubGroup membership represents the interest across the entire agency.

Interagency Advisory Board (IAB) – A coordination committee outside of the agency, to which the agency sends representatives, that provides the interface between the OMB and sponsoring Federal Government agencies. The IAB consists of Federal officials from contributing agencies and departments. The IAB shall:

a. Coordinate and leverage ongoing federal research, development, testing and evaluation (RDT&E) efforts to meet the HSPD-12 requirements as identified by OMB.

b. Solicit and coordinate mission support which includes activities such as organizational staff support, contributory funding, project sponsors, meetings, technical support, the IAB business cycle, and resulting products.

c. Meet to coordinate Federal requirements.

d. Attend general membership meetings.

4. Execution.

The Working Group shall conduct its mission during weekly meetings. The co-chair will provide a meeting agenda no later than three business days prior to the weekly meeting. The co-chair will record the issues addressed during each weekly meeting.