AUDIT REPORT

Audit of NRC's Implementation of
HSPD-12 Phase 2

OIG-11-A-09 March 30, 2011

All publicly available OIG reports (including this report) are accessible through
NRC's Web site at:
http:/www.nrc.gov/reading-rm/doc-collections/insp-gen/

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

OFFICE OF THE
INSPECTOR GENERAL

March 30, 2011

MEMORANDUM TO: R. William Borchardt
Executive Director for Operations

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

SUBJECT: AUDIT OF NRC'S IMPLEMENTATION OF HSPD-12
PHASE 2 (OIG-11-A-09)

Attached is the Office of the Inspector General's (OIG) audit report titled, *Audit of NRC's Implementation of HSPD-12 Phase 2.*

The report presents the results of the subject audit. Informal comments provided by agency management at the March 21, 2011, exit conference have been incorporated, as appropriate, into this report.

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 followup as stated in Management Directive 6.1.

We appreciate the 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 415-5915 or Beth Serepca, Security and Information Team Leader, at 415-5911.

Attachment: As stated

Electronic Distribution

Edwin M. Hackett, Executive Director, Advisory Committee
on Reactor Safeguards
E. Roy Hawkens, Chief Administrative Judge, Atomic Safety
and Licensing Board Panel
Stephen G. Burns, General Counsel
Brooke D. Poole, Director, Office of Commission Appellate Adjudication
James E. Dyer, Chief Financial Officer
Margaret M. Doane, 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
R. William Borchardt, Executive Director for Operations
Michael F. Weber, Deputy Executive Director for Materials, Waste,
Research, State, Tribal, and Compliance Programs, OEDO
Darren B. Ash, Deputy Executive Director
for Corporate Management, OEDO
Martin J. Virgilio, Deputy Executive Director for Reactor
and Preparedness Programs, OEDO
Mary C. Muessle, Assistant for Operations, OEDO
Kathryn O. Greene, Director, Office of Administration
Patrick D. Howard, Director, Computer Security Office
Roy P. Zimmerman, Director, Office of Enforcement
Charles L. Miller, Director, Office of Federal and State Materials
and Environmental Management Programs
Cheryl L. McCrary, Director, Office of Investigations
Thomas M. Boyce, Director, Office of Information Services
Miriam L. Cohen, Director, Office of Human Resources
Michael R. Johnson, Director, Office of New Reactors
Catherine Haney, Director, Office of Nuclear Material Safety
and Safeguards
Eric J. Leeds, Director, Office of Nuclear Reactor Regulation
Brian W. Sheron, Director, Office of Nuclear Regulatory Research
Corenthis B. Kelley, Director, Office of Small Business and Civil Rights
James T. Wiggins, Director, Office of Nuclear Security
and Incident Response
William M. Dean, Acting Regional Administrator, Region I
Victor M. McCree, Regional Administrator, Region II
Mark A. Satorius, Regional Administrator, Region III
Elmo E. Collins, Jr., Regional Administrator, Region IV

EXECUTIVE SUMMARY

BACKGROUND

HSPD-12 Requirements and Supporting Guidance for Federal Agencies

Homeland Security Presidential Directive 12 (HSPD-12) is a Presidential directive issued in August 2004. HSPD-12 states that it is national policy to "enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy" by establishing common identification standards for all Federal Government employees and contractors.[1] Further, HSPD-12 directs executive branch agencies to use standardized identification to gain physical access to Federal facilities and logical access to Federal information systems. As a Federal executive branch agency,[2] the U.S. Nuclear Regulatory Commission (NRC) is required to comply with HSPD-12 requirements.

The Office of Management and Budget (OMB) is responsible for issuing implementation guidance and ensuring Federal agencies' compliance with this guidance. OMB is also responsible for ensuring agency compliance with technical standards issued by the Secretary of Commerce. The National Institute of Standards and Technology (NIST)—an organization within the Department of Commerce—established basic technical standards in Federal Information Processing Standards Publication 201 (FIPS 201).[3]

[1] Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors,* August 27, 2004.

[2] Title 5 U.S. Code §105.

[3] Federal Information Processing Standards Publication 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, National Institute of Standards and Technology, March 2006.

FIPS 201 prescribes standards for verifying the identities of Federal employees and contractors,[4] issuing identification cards known as Personal Identity Verification (PIV) cards,[5] and managing data systems to support use of PIV cards.

Identity, Credential, and Access Management

Use of PIV cards is a basic element of a broader Federal Government initiative called Identity, Credential, and Access Management (ICAM), which aims to carry out specific provisions as well as the full intent of HSPD-12. ICAM programs have two main areas of operations: physical access control systems (PACS), which provide physical security at Federal facilities, and logical access control systems (LACS), which address the security of Federal computer networks.

HSPD-12 Implementation at NRC

NRC's Office of Administration (ADM) has primary responsibility for PACS implementation, including installation and maintenance of PIV card readers that control access at doors and other entry points at NRC facilities. At the end of this audit, NRC had completed installation of PIV card readers and the supporting data system within headquarters buildings. However, ADM staff told auditors that PACS deployment at NRC regional offices was ongoing and would likely continue through the first half of calendar year 2011.

NRC's Office of Information Services (OIS) provides information technology support for PACS, and has primary responsibility for forthcoming efforts to implement LACS at employees' computer workstations. To implement LACS, NRC will equip employee workstations with PIV card readers, and the cards will authenticate users to NRC's

[4] FIPS 201 refers to this process as identity proofing.

[5] Specifically, FIPS 201 describes PIV card elements, system interfaces, and security controls required to securely store, process, and retrieve identity credentials from the PIV card. Physical card characteristics, storage media, and data elements that make up identity credentials are specified in this standard.

network in lieu of multiple currently required application-specific passwords. OIS has started a pilot LACS program and expects to begin implementing the technology agencywide by the end of calendar year 2011.[6]

PURPOSE

The audit objective was to assess whether NRC has effectively implemented its ICAM programs.

RESULTS IN BRIEF

NRC completed implementation of the PACS portion of its ICAM program at headquarters facilities during calendar year 2010, and expects to conclude this work at regional offices during the first half of calendar year 2011. All NRC staff and contractors eligible for the new PIV identification cards required by HSPD-12 have obtained these cards, and NRC continues to integrate PIV card technology with physical security upgrades at its facilities. Further, NRC has begun piloting the use of LACS at employees' computer workstations to enhance network security and simplify the log-in process. Based on NRC's experience in transitioning to the new PACS technology, OIG identified opportunities to facilitate the NRC's LACS implementation through improved employee outreach and training.

RECOMMENDATIONS

This report makes recommendations to facilitate NRC's adoption of new information technology required for logical access control systems.

AGENCY COMMENTS

At an exit conference on March 21, 2011, agency management stated their general agreement with the finding and recommendations in this report. Agency management also provided supplemental information that has been incorporated into this report. As a result, the agency opted not to provide formal comments for inclusion in this report.

[6] Two NRC computer applications—the National Source Tracking System and the Safeguards Information Local Area Network and Electronic Safe—already employ LACS technology.

ABBREVIATIONS AND ACRONYMS

ADM	Office of Administration
HSPD-12	Homeland Security Presidential Directive 12
ICAM	Identity, Credential, and Access Management
FIPS	Federal Information Processing Standards
FY	fiscal year
LACS	Logical Access Control System
NIST	National Institute of Standards and Technology
NRC	U.S. Nuclear Regulatory Commission
OIG	Office of the Inspector General
OIS	Office of Information Services
OMB	Office of Management and Budget
PACS	Physical Access Control System
PIV	Personal Identity Verification

TABLE OF CONTENTS

APPENDIX

I. BACKGROUND

HSPD-12 Requirements and Supporting Guidance for Federal Agencies

Homeland Security Presidential Directive 12 (HSPD-12) is a Presidential directive issued in August 2004. HSPD-12 states that it is national policy to "enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy" by establishing common identification standards for all Federal Government employees and contractors.[7] Further, HSPD-12 directs executive branch agencies to use standardized identification to gain physical access to Federal facilities and logical access to Federal information systems. As a Federal executive branch agency,[8] the U.S. Nuclear Regulatory Commission (NRC) is required to comply with HSPD-12 requirements.

The Office of Management and Budget (OMB) is responsible for issuing implementation guidance and ensuring Federal agencies' compliance with this guidance. OMB is also responsible for ensuring agency compliance with technical standards issued by the Secretary of Commerce. The National Institute of Standards and Technology (NIST)—an organization within the Department of Commerce—established basic technical standards in Federal Information Processing Standards Publication 201 (FIPS 201).[9]

Personal Identity Verification

FIPS 201 prescribes standards for verifying the identities of Federal employees and contractors,[10] issuing identification cards known as

[7] Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors,* August 27, 2004.

[8] Title 5 U.S. Code §105.

[9] Federal Information Processing Standards Publication 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, National Institute of Standards and Technology, March 2006.

[10] FIPS 201 refers to this process as identity proofing.

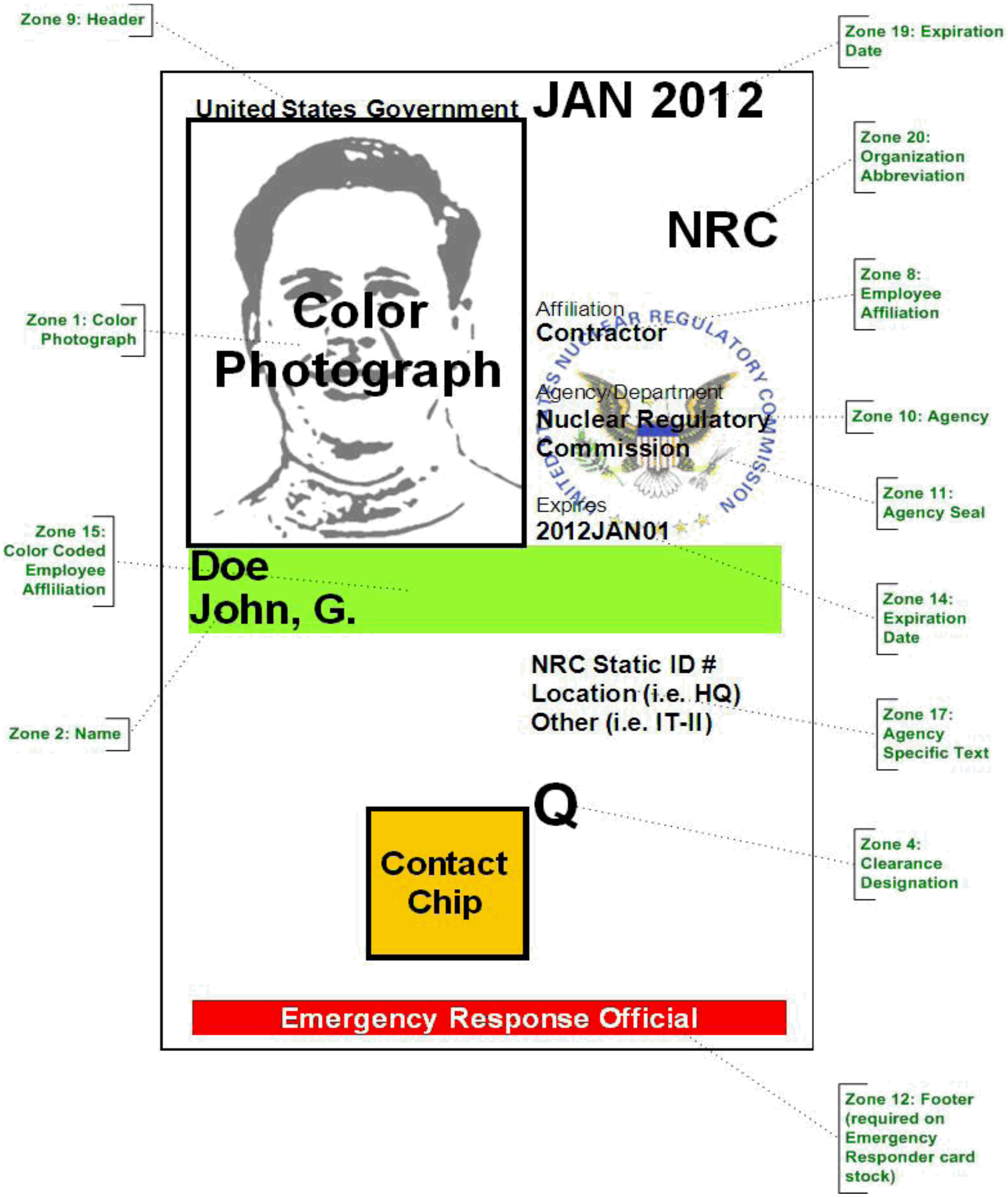
Personal Identity Verification (PIV) cards,[11] and managing data systems to support use of PIV cards. PIV cards are personalized with information unique to each employee. The surface of each PIV card shows an employee's photograph, name, agency, and affiliation (e.g., contractor, military, or civilian employee). PIV cards also store electronic information[12] that is transmitted via card readers to data servers, which use this information to confirm an employee's identity and access rights. The physical access PIV card readers are contactless, meaning they can read the information contained in PIV cards when an employee places his/her PIV card on or near a reader's surface.[13] Physical access PIV card readers are typically connected to door locks, which are locked as their default setting but unlock briefly when employees with appropriate access rights apply their PIV cards to the readers. Security officers may also use mobile, hand-held PIV card readers to control access in areas without fixed entry points, such as hallways and elevator banks. Figures 1 and 2 illustrate a sample NRC PIV card, and describe the data elements and their placement on the front and back sides as required by FIPS 201.

[11] Specifically, FIPS 201 describes PIV card elements, system interfaces, and security controls required to securely store, process, and retrieve identity credentials from the PIV card. Physical card characteristics, storage media, and data elements that make up identity credentials are specified in this standard.

[12] Electronic information stored on PIV cards includes the Cardholder Unique Identifier; Personal Identification Number; two biometric fingerprint templates; and authentication data including the PIV authentication key, card authentication key, digital signature key, and key management key. PIV cards themselves do not store personally identifiable information, such as social security numbers.

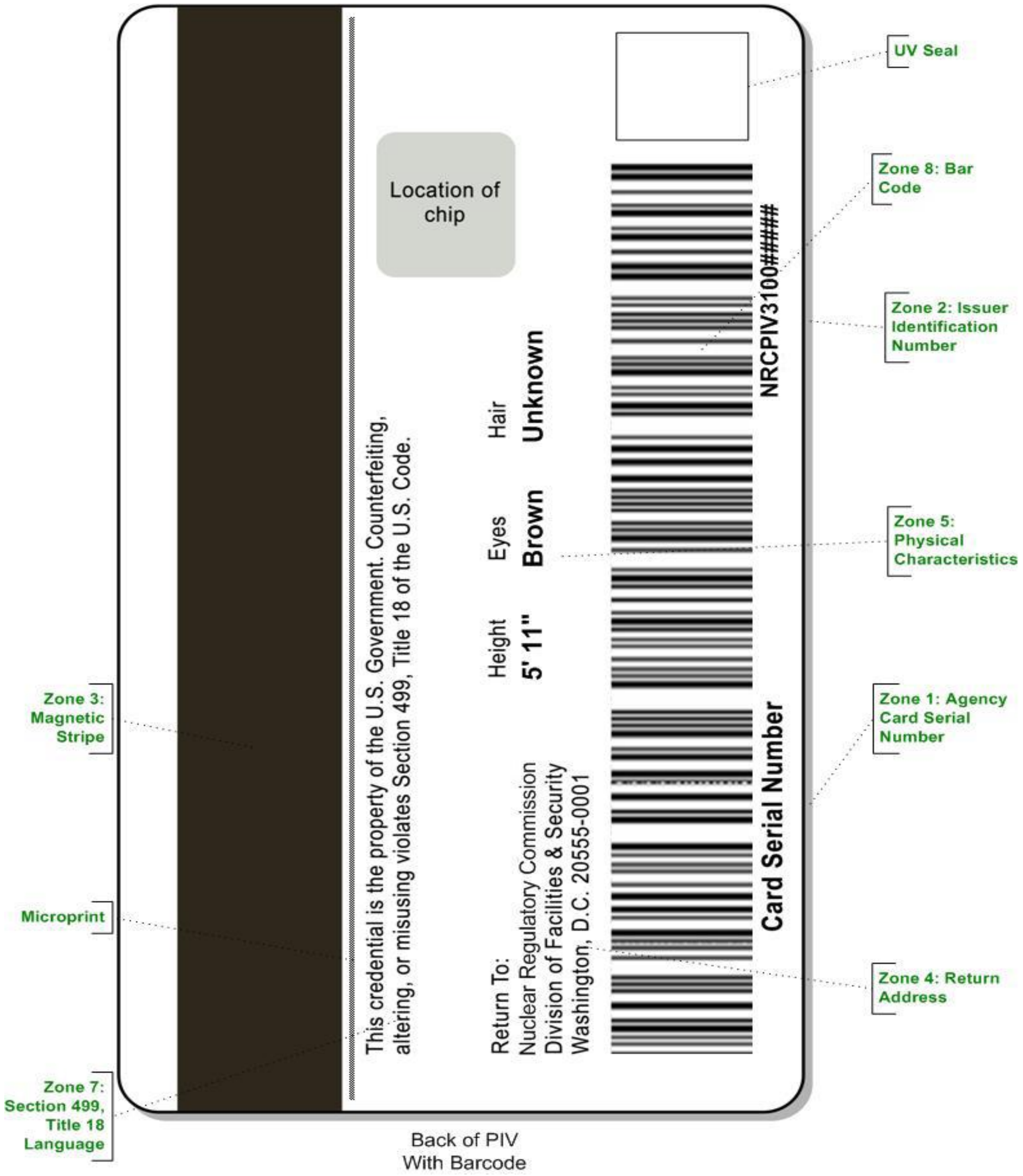
[13] Before NRC adopted PIV cards, the agency used identification cards that relied upon physical contact between the card and card reader interface to unlock doors.

Figure 1: Sample NRC PIV Card (Front View)



Source: NRC

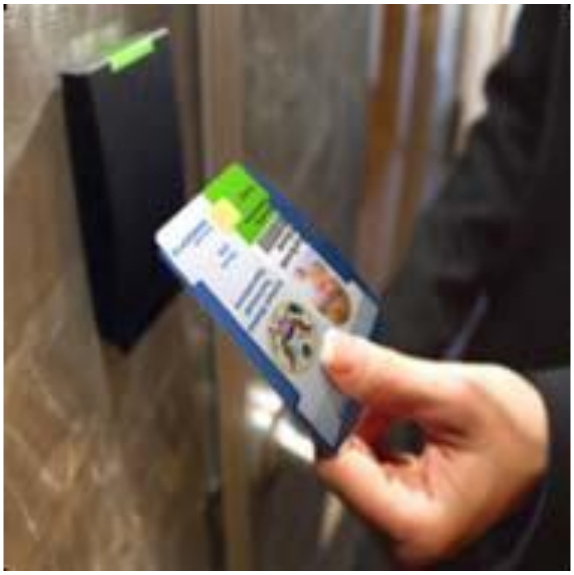
Figure 2: Sample NRC PIV Card (Back View)


UV Seal
Zone 8: Bar Code
Zone 2: Issuer Identification Number
Zone 5: Physical Characteristics
Zone 1: Agency Card Serial Number
Zone 4: Return Address
Zone 3: Magnetic Stripe
Microprint
Zone 7: Section 499, Title 18 Language
Location of chip
This credential is the property of the U.S. Government. Counterfeiting, altering, or misusing violates Section 499, Title 18 of the U.S. Code.
Height
5' 11"
Eyes
Brown
Hair
Unknown
Return To:
Nuclear Regulatory Commission
Division of Facilities & Security
Washington, D.C. 20555-0001
NRCPIV3100####
Card Serial Number
Back of PIV
With Barcode

Source: NRC

Figure 3 illustrates how PIV cards and fixed card readers are used to unlock a door (note the green light on the card reader indicating that the adjacent door is temporarily unlocked).

Figure 3: Photograph of PIV Card Use for Physical Access



Source: NRC

NRC began issuing PIV cards to employees and contractors during early 2010,[14] and requiring use of PIV cards for physical access to NRC headquarters facilities beginning in July 2010.[15] As of September 1, 2010, NRC had issued PIV cards to 4,331 eligible staff and 1,236 eligible contractors. This represents 100 percent of NRC and contractor personnel with completed background checks who were eligible to obtain PIV cards.

[14] In accordance with OMB guidance, Federal agencies must conduct background reviews of all employees and contractors who are to be issued PIV cards.

[15] Installation of PIV card readers and supporting data systems at some non-headquarters facilities was still underway at the conclusion of this audit. See Appendix, "Scope and Methodology."

NRC's Identity, Credential, and Access Management Programs

Use of PIV cards is a basic element of a broader Federal Government initiative called Identity, Credential, and Access Management (ICAM), which aims to carry out specific provisions as well as the full intent of HSPD-12. ICAM programs have two main areas of operations: physical access control systems (PACS), which provide physical security at Federal facilities, and logical access control systems (LACS), which address the security of Federal computer networks. NRC staff meet on a regular basis with representatives from other Federal agencies to share information and keep apprised of changing guidance that can impact agencies' respective ICAM programs.

NRC's Office of Administration (ADM) has primary responsibility for PACS implementation, including installation and maintenance of PIV card readers that control access at doors and other entry points at NRC facilities. At the end of this audit, NRC had completed installation of PIV card readers and the supporting data system within headquarters buildings. However, ADM staff said that PACS deployment at NRC regional offices was ongoing and would likely continue through the first half of calendar year 2011.

NRC's Office of Information Services (OIS) provides information technology support for PACS, and has primary responsibility for forthcoming efforts to implement LACS at employees' computer workstations. To implement LACS, NRC will equip employee workstations with PIV card readers, and the cards will authenticate users to NRC's network in lieu of multiple, currently required application-specific passwords. A primary objective of LACS is to enhance computer network security by using digital certificates to verify the identity of network users in lieu of multiple passwords, which can be forgotten by employees and are more easily compromised. In addition, LACS may slightly enhance workplace efficiency because NRC employees will have fewer passwords to memorize and change on a routine basis. OIS has started a pilot LACS program and expects to begin implementing the technology agencywide by the end of calendar year 2011.[16] Figure 4 shows an illustration of a computer workstation PIV card reader.

[16] Two NRC computer applications—the National Source Tracking System and the Safeguards Information Local Area Network and Electronic Safe—already employ LACS technology.

Figure 4: Computer Workstation PIV Card Reader

Source: NRC

NRC spent approximately $3.7 million over the Fiscal Year (FY) 2007-2010 period on PACS implementation costs such as hardware, software, data system certification and accreditation, and labor. NRC spent approximately $2.4 million in FY 2010 for LACS implementation. NRC expects to spend approximately $1.3 million over the FY 2011-2012 period to operate and maintain PACS equipment, and to integrate it with LACS infrastructure.

II. PURPOSE

The audit objective was to assess whether NRC has effectively implemented its ICAM programs. See the report appendix for information on the audit scope and methodology.

III. FINDING

NRC completed implementation of the PACS portion of its ICAM program at headquarters facilities during calendar year 2010, and expects to conclude this work at regional offices during the first half of calendar year 2011. All NRC staff and contractors eligible for the new PIV identification cards required by HSPD-12 have obtained these cards, and NRC continues to integrate PIV card technology with physical security upgrades at its facilities. Further, NRC has begun piloting the use of LACS at employees' computer workstations to enhance network security and simplify the log-in process. Based on NRC's experience in transitioning to the new PACS technology, the Office of the Inspector General (OIG) identified opportunities to improve the transition to LACS technology. This report makes recommendations to enhance employee outreach in preparation for LACS implementation at NRC.

NRC Can Improve Employee Outreach and Training in Preparation for LACS Implementation

Effective employee outreach and training are important steps in managing technological and procedural changes at organizations. NRC conducted limited outreach activities in preparation for PACS implementation. However, additional outreach activities occurred several months after the use of PIV cards became mandatory for physical access at NRC headquarters. This delay occurred for two main reasons. First, NRC lacked a communications plan for educating employees about PACS and for coordinating outreach activities with PACS implementation schedules. Second, some policies and procedures for using PACS equipment—i.e., "use case" [17] policies and procedures—were still evolving after the equipment's use became mandatory at NRC headquarters. This had relatively minor effects on employee attitudes toward and understanding of PACS use. However, NRC's forthcoming LACS implementation will significantly impact policies and procedures for accessing NRC computer networks. Consequently, NRC employees must have a clear understanding of these policies and procedures to avoid disruptions that could adversely affect employee productivity.

[17] "Use case" is a software and systems engineering term that describes how information technology will function in response to user behavior. In short, a "use case" describes "who" can do "what" with information technology in specific scenarios or conditions.

Outreach and Training Are Key To Managing Technological and Procedural Change

Effective employee outreach and training are important steps in managing technological and procedural changes at organizations. A draft version of ICAM guidance recently circulated by the Federal Chief Information Officers Council to NRC and other Federal agencies identifies outreach as a key PACS implementation activity. Specifically, outreach “involves actively communicating to users that a new access control system is being deployed, the benefits and efficiencies that users can expect, and any steps necessary to begin using the new system. Informational materials need to clearly communicate the right message to the appropriate audience.” The draft ICAM guidance also describes end user training as a related and highly important step. In particular, training materials “should be created with the end user in mind and *training should be completed prior to PACS deployment to ensure that users are capable of accessing facilities without undue disruption to the agency’s mission*.” The draft ICAM guidance makes similar recommendations for LACS implementation, and emphasizes LACS training “*prior to LACS deployment* to ensure that users are capable of accessing protected resources without undue disruption to the agency’s mission.” [Italics added for emphasis.]

PACS Implementation Had Limited Outreach and Training

NRC conducted limited outreach activities and no formal user training in preparation for PACS implementation. NRC's primary means for educating staff about PACS were e-mail announcements, and two “Town Hall” meetings during which NRC staff addressed NRC employees’ questions about HSPD-12 as well as headquarters building construction and renovation. NRC staff produced a PowerPoint presentation explaining PIV cards’ purpose and use. However, this presentation appeared on the NRC Intranet in September 2010—approximately 2 months after NRC began requiring employees to badge in with their new PIV cards in July 2010. Similarly, NRC staff created placards to inform personnel about PIV cards, but the placards were undergoing management review in December 2010—approximately 5 months after PIV cards became mandatory for physical access to headquarters buildings.

NRC Lacked Communications and Training Plan in Preparation for PACS Implementation

NRC conducted limited outreach and training in preparation for PACS implementation for two reasons. First, NRC lacked a communications plan for educating employees about PACS through different media and coordinating outreach activities with PACS implementation schedules.

Second, some policies and procedures for using PACS equipment—i.e., "use case" policies and procedures—were still evolving after the equipment's use became mandatory. For example:

- Badge-in procedures changed after ADM staff realized that NRC employees were having difficulty placing their PIV cards properly on the card readers at pedestrian and vehicular entrances. In response, contract guards were instructed to take employees' PIV cards and badge them in.

- NRC activated new anti-tailgating sensors at select locations in September 2010, and required employees to follow specific anti-tailgating procedures.[18] However, ADM staff acknowledged during this audit that the procedures were provisional and subject to change based upon lessons learned following the deployment of the anti-tailgating equipment.

Although NRC could develop physical access "use case" policies after PACS became operational with minimal inconvenience to employees, the agency will not have this flexibility during LACS implementation. Unlike physical access procedures that allow for visual authentication and issuance of temporary identification cards, LACS will require a PIV card for employees to access NRC's networks from their workstations. For example:

1. If employees forget to bring their PIV cards to work, NRC must either develop a technical solution that enables them to access agency networks, or establish policies to account for lost work time.

[18] Anti-tailgating sensors are designed to detect individuals who follow others through doorways without applying PIV cards to the card readers.

2. Lost or stolen PIV cards present a different challenge since these circumstances require termination of a lost or stolen card. Employees must then obtain a new PIV card.

3. Some executive staff may be exempt from LACS policies; if so, NRC must specify the level of seniority that permits exemptions and apply this policy consistently across the agency.

Improved Outreach and Training Will Be Critical for LACS Implementation

Despite challenges in NRC's transition to new PACS technology, auditors found no material effect on NRC operations. Anecdotal evidence suggests some staff regard PIV cards as a minor inconvenience and do not understand NRC's requirements and conditions for PIV cards. Further, NRC staff said that a few PIV cards are damaged on a weekly basis through employee misuse.[19] Nevertheless, NRC's plans to deploy LACS technology will significantly impact policies and procedures for accessing NRC computer networks. NRC staff are working to address LACS "use cases," such as lost, stolen, or forgotten PIV cards, as well as employees who have multiple job roles and access rights parameters.[20] NRC management is aware of these and other "use case" challenges, but must ensure they are resolved prior to LACS implementation to avoid work-routine disruptions that could adversely affect employee productivity.

[19] PIV cards contain antennae coils to transmit data to contactless PIV card readers. These coils are fragile and cannot withstand repeated stress from flexing.

[20] At present, Federal PIV card security policies assume a principle of "one individual, one PIV card, one set of roles." However, an NRC employee may have limited user rights in some NRC network applications while maintaining broader administrative rights in one or more applications.

Further, NRC employees and managers across the agency must understand LACS policies and procedures so that employees are not inadvertently denied network access, and do not compromise NRC network security by inadvertently violating LACS "use case" policies.

IV. RECOMMENDATIONS

OIG recommends that the Executive Director for Operations:

1. Create and implement a LACS communication and outreach plan that targets NRC users through different media, and is coordinated with LACS deployment schedules.

2. Require one-time mandatory LACS policy and procedure training for all staff, managers, and contractors who require desktop access to NRC networks, and make this training available in an on-demand format.

3. Establish clear "use case" policies and procedures prior to LACS deployment.

V. AGENCY COMMENTS

At an exit conference on March 21, 2011, agency management stated their general agreement with the finding and recommendations in this report. Agency management also provided supplemental information that has been incorporated into this report. As a result, the agency opted not to provide formal comments for inclusion in this report.

Appendix

SCOPE AND METHODOLOGY

The audit objective was to assess whether NRC has effectively implemented its ICAM programs. To address the audit objective, OIG auditors attended briefings presented by NRC staff, NRC contractors, and representatives from other Federal agencies. OIG auditors toured facilities at the NRC headquarters complex, the NRC Region II office, and the NRC Technical Training Center. During these tours, OIG auditors observed new PACS equipment in use, tested it to ensure compliance with NRC security plans, and questioned NRC staff and contract security personnel about the equipment. OIG auditors also toured a contractor facility that manufactures PIV cards for NRC and other Federal clients. Further, OIG auditors conducted multiple interviews of NRC staff representing ADM, OIS, and the Computer Security Office, as well as contractor personnel who provide technical support to NRC.

OIG auditors reviewed pertinent guidance, including:

- *HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors,* August 27, 2004.

- 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.

- FIPS 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors,* March 2006.

- NIST SP 800-116, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS),* November 2008.

- *Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance*, *Part B: Implementation Guidance Initial Phase 1 ICAM Release Draft,* November 19, 2010.

- Orders for NRC headquarters contract security personnel.

In addition, OIG auditors reviewed contract documentation, budget data, and staff manpower data related to PACS and LACS implementation, as well as Commission papers and other relevant internal planning documents. OIG auditors also reviewed documentation of efforts to ensure PACS data system compliance with Federal information system security requirements.

OIG conducted this performance audit at NRC headquarters from September 2010 through March 2011 in accordance with generally accepted Government auditing standards. Those standards require the audit to be planned and performed with the objective of obtaining sufficient, appropriate evidence to provide a reasonable basis for any findings and conclusions based on the stated audit objective. OIG believes that the evidence obtained provides a reasonable basis for the report findings and conclusions based on the audit objective. OIG reviewed and analyzed internal controls related to the audit objective. Throughout the audit, auditors were aware of the possibility or existence of fraud, waste, or misuse in the program. The audit was conducted by Beth Serepca, Team Leader; Paul Rades, Audit Manager; and Gail Butler, Analyst.