

APRIL 27, 2009

AUDIT REPORT

OFFICE OF AUDITS

NASA'S PROCESSES FOR PROVIDING PERSONAL
IDENTITY VERIFICATION (PIV) CARDS
WERE NOT COMPLETELY EFFECTIVE
IN MEETING FEDERAL REQUIREMENTS

OFFICE OF INSPECTOR GENERAL



National Aeronautics and
Space Administration

Final report released by:

/s /

Evelyn R. Klemstine
Assistant Inspector General for Auditing

Acronyms

AIMO	Agency Identity Management Official
ATO	Authorization to Operate
CBACS	Common Badging and Access Control System
CIO	Chief Information Officer
DAA	Designated Accreditation Authority
DATO	Denial of Authorization to Operate
FIPS	Federal Information Processing Standards
HSPD-12	Homeland Security Presidential Directive 12
IATO	Interim Authorization to Operate
IT	Information Technology
NID	NASA Interim Directive
NIST	National Institute of Standards and Technology
NPD	NASA Policy Directive
NPR	NASA Procedural Requirements
OIMO	Organization Identity Management Official
OMB	Office of Management and Budget
OSPP	Office of Security and Program Protection
PIV	Personal Identity Verification
SATERN	System for Administration, Training, and Educational Resources for NASA
SP	Special Publication

OVERVIEW

NASA'S PROCESSES FOR PROVIDING PERSONAL IDENTITY VERIFICATION (PIV) CARDS WERE NOT COMPLETELY EFFECTIVE IN MEETING FEDERAL REQUIREMENTS

The Issue

On August 27, 2004, the President signed Homeland Security Presidential Directive 12 (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and Contractors." HSPD-12 mandated that all Federal agencies develop and deploy an identification verification system to provide uniform employee and contractor personal identity verification (PIV) credentials that could be used reciprocally among all Federal Government agencies. To support reciprocity, the National Institute of Standards and Technology (NIST) developed a formal accreditation process for establishing the reliability of issuers of PIV credentials. HSPD-12 guidance states the PIV credentials are to be issued only by providers whose reliability has been verified by an official assessment and accreditation process and that all Federal agencies perform background investigations and begin issuing HSPD-12 compliant PIV cards to employees and contractors by October 2007.

Before the enactment of HSPD-12, NASA had already begun developing an Agency-wide common badging and access control system (CBACS). To comply with HSPD-12, NASA decided to integrate HSPD-12 requirements into the Agency's ongoing common badging and access control efforts. In July 2006, NASA established an HSPD-12 implementation office to coordinate the integration effort. We conducted this audit to evaluate the effectiveness of NASA's processes for developing and issuing HSPD-12 compliant PIV cards. We gathered data and information from all NASA locations¹ on the processes used to request, sponsor, authorize, and issue PIV cards. Details of the audit's scope and methodology are in Appendix A.

Results

As of January 9, 2009, NASA had issued more than 70,000 PIV cards to staff and contractors, more than 98 percent of the PIV cards NASA planned to issue, from a PIV card issuer that had not been accredited because NASA did not fully comply with Federal guidance. While NASA properly assessed the PIV card issuer for satisfaction of Federal requirements at both organization and facility levels, found deficiencies, and developed a

¹ The Jet Propulsion Laboratory was not included in our audit because of pending litigation related to the gathering of PIV data.

corrective action plan in accordance with Federal guidance, the Agency did not monitor corrective actions to ensure that identified deficiencies were corrected nor initiate timely reassessment. If the reassessment of the PIV card issuer reveals that significant deficiencies continue to exist and those deficiencies affect the integrity of the PIV cards, NASA could be required to discontinue PIV card issuer operations and reissue its PIV cards, which we estimate could cost a minimum of \$1 million.

NASA's noncompliance with Federal guidance resulted from the lack of a project management plan for the Agency's transition to HSPD-12 compliant PIV cards. For example, NASA did not establish an implementation office to plan and coordinate project integration until July 2006—2 years after HSPD-12 was signed and 3 months before the deadline for agencies to begin issuing HSPD-12 compliant identity cards. Also, NASA did not comply with its own policy on incorporating new requirements into ongoing projects nor conduct a gap analysis to ensure that the ongoing common badging and access control projects incorporated HSPD-12 requirements. In an effort to meet established deadlines, NASA implemented processes and systems that had not been adequately planned and, as a result, developed the system for producing PIV cards but did not complete the accreditation process for ensuring that the system subcomponents met Federal requirements for HSPD-12.

Although we did not identify any instances of PIV cards being issued to unauthorized individuals, we did find that NASA did not fully develop internal controls needed to efficiently and effectively implement HSPD-12. Specifically, we found that NASA did not establish sufficient controls to ensure that personnel assigned PIV roles fulfilled training requirements before performing PIV duties and to ensure that personnel used consistent methods for issuing temporary credentials to non-NASA Federal employees. In addition, NASA's PIV system processes did not provide a comprehensive audit trail for identifying errors and irregularities. If the deficiencies identified are not corrected, the risk of NASA issuing PIV cards to individuals who have no legitimate need to access NASA's facilities or systems could be increased.

Management Action

During the audit, NASA management took actions to address our preliminary findings that PIV card issuer oversight responsibilities were not appropriately safeguarded in accordance with Federal guidance and that internal controls were insufficient to prevent one individual from performing both sponsoring and authorizing functions of issuing a PIV card. On January 12, 2009, the Senior Agency Official for HSPD-12 reassigned the PIV card issuer oversight roles to two individuals. At the two Centers where one individual both sponsored and authorized the issuance of a PIV card, both Centers reprocessed those PIV card requests to comply with the separation of duties requirement and PIV officials upgraded the PIV system adding controls to prevent one individual from performing conflicting PIV duties. Therefore, we did not include recommendations to further address PIV card issuer oversight responsibilities.

We do recommend, however, that the Assistant Administrator for the Office of Security and Program Protection (1) determine if the designated accreditation authority for the PIV card issuer should issue a denial of authorization to operate if subsequent reassessment results determine that significant deficiencies for the PIV card issuer continue to exist.

We also recommend that, for future information technology (IT) projects, the Chief Information Officer and the Assistant Administrator for the Office of Security and Program Protection (2) follow Agency procedural requirements to plan and manage the development of IT projects and (3) require system owners to conduct and document a gap analysis when Federal directives and requirements impact IT project development.

We further recommend that the Assistant Administrator for the Office of Security and Program Protection (4) notify all personnel involved in the PIV process of the requirement to complete training prior to performing their PIV duties and add the training requirement to the individuals' NASA learning plan, (5) develop and implement NASA policies for issuing temporary badges and HSPD-12 compliant PIV cards to non-NASA Federal employees assigned to NASA locations and establish and include appropriate expiration date guidelines for temporary badges, and (6) modify the PIV system to increase data visibility by modifying the system and incorporating a single-audit infrastructure that pulls the necessary audit trail data from the PIV system subcomponents.

In response to a draft of this report issued March 20, 2009, the Assistant Administrator for the Office of Security and Program Protection and the Chief Information Officer concurred with our recommendations. However, management's comments on Recommendations 2 and 3 were not responsive because they did not detail the actions the Agency would take to ensure future IT projects would be planned and managed in accordance with NASA project management policy; nor did the comments provide details on how the Agency plans to ensure that a gap analysis is conducted and documented when changes in Federal directives and requirements have an impact on ongoing IT projects. Therefore, Recommendations 2 and 3 remain unresolved. We request that the Assistant Administrator for the Office of Security and Program Protection and the Chief Information Officer provide additional comments in response to this final report by May 26, 2009.

CONTENTS

INTRODUCTION

Background	1
Objectives	3

RESULTS

Finding A: Noncompliance with Federal Guidance Could Compromise Issuance of NASA's PIV Cards	4
Finding B: Lack of Internal Controls Hampered Effective HSPD-12 Implementation	13
Finding C: NASA Responds to Issues Related to Role Separations	19

APPENDIX A

Scope and Methodology	23
Review of Internal Controls	24
Prior Coverage	24

APPENDIX B

Management Comments	25
---------------------	----

APPENDIX C

Report Distribution	28
---------------------	----

INTRODUCTION

Background

In 2002, NASA's Office of Security and Program Protection (OSPP) created the Smart Card Project and the Identity Management System (IDMS) to develop a common credential for granting access to NASA's physical and logical resources. As part of the development process, OSPP surveyed all NASA locations and found that each location had a different access control system. Thus, in 2004, OSPP and the NASA Chief Information Officer (CIO) determined that NASA needed a common badging and access control system (CBACS), and the Smart Card Project evolved into the CBACS project. As described on the NASA CIO Web site, CBACS is "a system of records to document, track, manage, analyze, produce a NASA badge that is verifiable, identifiable, durable and can be used to access NASA resources (physical and logical)." CBACS uses Central Card Management System and IDMS for identity management and issuance of smart cards to all NASA civil servants, contractors, foreign nationals, and visitors. The system also uses Enterprise Physical Access Control System (E-PACS) and the physical smart card reader.

On August 27, 2004, the President signed HSPD-12, which requires all Federal agencies to develop and deploy a standard, common, and reliable identification verification system for employees and contractors to use Government-wide to increase the security of Federal facilities and information systems. The implementation memorandum, issued by the Office of Management and Budget (OMB) on August 5, 2005,² tasked the Department of Commerce, through NIST, with developing standards for secure and reliable credentials for Government employees and contractors. The memorandum cited NIST's Federal Information Processing Standards (FIPS) 201 as the standard guidance for implementing the directive. FIPS 201-1, "Personal Identity Verification (PIV) of Federal Employees and Contractors," March 2006, defines the technical requirements for the common credential as

- issued based on sound criteria for verifying an individual employee's identity;
- resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation;
- rapidly authenticated electronically; and
- issued only by providers whose reliability has been established by an official accreditation process.

² OMB, "Implementation of Homeland Security Presidential Directive (HSPD)-12 – Policy for a Common Identification Standard for Federal Employees and Contractors" (M-05-24, August 5, 2005).

NIST also developed Special Publication (SP) 800-79,³ “Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations,” July 2005. In June 2008, NIST updated the publication and issued it as SP 800-79-1, “Guidelines for the Accreditation of Personal Identity Verification Card Issuers” to outline the requirements for assessing and accrediting providers of HSPD-12-compliant identification cards. NIST SP 800-79-1 also identifies the roles and responsibilities for ensuring compliance with HSPD-12 requirements:

- Senior Authorizing Official (SAO) is responsible for all PIV card issuer⁴ operations, has budgetary control, provides oversight, develops policy, and has authority over all functions and services provided by the PIV card issuer.
- Designated Accreditation Authority (DAA) has the authority to review all assessments of a PIV card issuer and its facilities and to accredit the PIV card issuer as required by HSPD-12. Through accreditation, the DAA accepts responsibility for the operation of the PIV card issuer at an acceptable level of risk to the organization. The SAO can also fulfill the role of the DAA.
- Organization Identity Management Official (OIMO) (at NASA, Agency Identity Management Official or AIMO) is responsible for implementing policies of the organization, assuring that all specified procedures of the PIV card issuer are being performed reliably, and providing guidance and assistance to the PIV card issuer facilities. The AIMO implements and manages the PIV card issuer operations plan; ensures that all PIV card issuer roles are filled with capable, trustworthy, knowledgeable, and trained staff; makes certain that all PIV card issuer services, equipment, and processes meet FIPS 201-1 requirements; monitors and coordinates activities with PIV card issuer facility manager(s); and supports the accreditation process. NIST SP 800-79-1 states that the AIMO cannot fulfill the role of the DAA.

NASA management decided that to comply with the presidential mandate to develop a reliable and secure credential, NASA would incorporate the HSPD-12 and FIPS 201 requirements into the development of CBACS and other ongoing projects. Development of the NASA PIV system to implement HSPD-12 requirements was a collaborative effort between OSPP, the NASA CIO, and the Marshall Space Flight Center (Marshall) CIO who was responsible for developing the system. In July 2006, NASA issued Program Decision Memorandum Number 28, establishing an Agency-level HSPD-12 Project Office tasked with determining Agency requirements for, and managing implementation of, HSPD-12. The project office reported directly to the Deputy Administrator on a monthly basis. The memorandum also stated that implementing HSPD-12 requirements, estimated to cost between \$112 and \$160 million, would be funded from existing Agency institutional and program budgets. On May 24, 2007, NASA issued NASA Interim

³ In revising SP 800-79 to SP 800-79-1, the title wording changed from certification and accreditation of the PIV card issuer to assessment and accreditation of the PIV card issuer.

⁴ NIST SP 800-79-1 uses the acronym “PCI” rather than PIV card issuer, the term used in this report.

Directive (NID), “Personal Identity Verification (PIV) Policy and Procedures,” to augment NASA Procedural Requirements (NPR) 1600.1, “NASA Security Program Procedural Requirements,” November 3, 2004, which establishes the policy for creating and issuing federally compliant credentials. As of January 9, 2009, NASA had issued 72,024 PIV cards (about 98.5 percent of the total number of cards the Agency intended to issue for employees and contractors).

NASA’s PIV system consists of several major components including IdMAX, the component that manages information flow and process status among all components and maintains the state of the entire PIV card process. The PIV system uses other interrelated NASA systems including CBACS, the Federal Personnel Payroll System, and the Workforce Transformation Tracking System. The PIV system also uses data from the Office of Personnel Management’s Electronic Questionnaire for Investigations Processing and Personnel Investigations Processing System.

The architecture to support logical access controls of NASA systems is still evolving. Generally, logical access allows authorized employees to access NASA resources as determined necessary by the appropriate system and network managers. At some point in the future, a NASA identification badge holder’s information will be updated to include access control information that can be transmitted to the NASA server for authentication and active directory services. When a user wants to access any protected logical resource—including facilities or computers—the user will insert his/her badge and enter the associated personal identification number. Then the protected resource verifies the user’s identity on the badge, checks for revocation, and consults the appropriate data store or directory service to determine whether to allow the badge holder access to the logical resource.

Objectives

The overall objective was to evaluate the effectiveness of NASA’s processes for developing and issuing HSPD-12 compliant PIV cards. Specifically, we evaluated the

- adequacy of NASA’s plans for managing the transition to PIV cards that are compliant with HSPD-12;
- assessment and accreditation of the PIV card issuer; and
- processes for issuance and maintenance of PIV cards.

We also reviewed internal controls as they relate to the overall objective. See Appendix A for details of the audit’s scope and methodology, our review of internal controls, and a list of prior audit coverage.

FINDING A: NONCOMPLIANCE WITH FEDERAL GUIDANCE COULD COMPROMISE ISSUANCE OF NASA'S PIV CARDS

NASA managers did not follow NIST guidance and interim authorization to operate (IATO) requirements for assessing and accrediting the PIV card issuer. Specifically, NASA did not monitor deficiencies found during the initial PIV card issuer assessment and did not initiate a timely reassessment to accredit the card issuer. Instead, the Agency issued the PIV card issuer a yearlong IATO and two consecutive extensions to the IATO, allowing the card issuer to operate without being accredited. NASA did not comply with Federal guidance because of the lack of a project management plan to effectively prepare for implementing HSPD-12 credentialing requirements. NASA did not develop an overall implementation plan nor conduct a gap analysis to determine what requirements CBACS and other ongoing projects lacked that HSPD-12 mandated. In addition, NASA management directed implementation staff to meet the OMB deadline to begin issuing HSPD-12 compliant PIV cards. As a result, the Agency issued 98.5 percent of the PIV cards it expected to issue from a card issuer that had not been deemed reliable, as required by NIST. NASA could be required to discontinue PIV card issuer operations and reissue its PIV cards, which could cost NASA about \$1 million just for the card stock if the reassessment of the PIV card issuer reveals that significant deficiencies continue to exist and those deficiencies affect the integrity of the PIV cards.

Federal and NASA Guidance

Federal criteria specific to implementing HSPD-12 requirements is provided in FIPS 201-1, which focuses on the architecture and technical requirements for a common identification standard for Federal employees and contractors, and NIST SP 800-79-1, which focuses on assessment and accreditation of the PIV card issuer. Assessment is the process of gathering evidence of a PIV card issuer's satisfaction of the requirements of FIPS 201-1, at both organizational and facility levels. Accreditation is the decision to authorize the operation of a PIV card issuer once it has been established that the PIV card issuer has met the requirements of FIPS 201-1 and that risks regarding security and privacy are acceptable. NIST SP 800-79-1 provides a methodology for verifying that issuers of PIV cards are adhering to standards and implementation directives developed under HSPD-12 that involves drawing the PIV card issuer's accreditation boundary, evaluating the findings of all reliability assessments, and making a proper decision for accrediting the PIV card issuer. NIST SP 800-79-1 further notes that careful planning, preparation, and commitment of time, energy, and resources are required for the

assessment and accreditation, which involves agencies in creating the needed roles, assigning responsibilities, and developing an acceptable operations plan.

NASA identifies planning as a necessary structural element of project development. NASA Policy Directive (NPD) 2800.1, “Managing Information Technology,” March 23, 1998, notes that NASA’s policy is to plan for, acquire, manage, and use IT to accomplish NASA’s missions and programs efficiently, effectively, and securely. The policy also states that NASA should make measurable improvements by planning, budgeting, acquiring, and evaluating the performance of IT investments. NPR 2800.1, “Managing Information Technology,” September 17, 1998, also establishes policies for planning, acquiring, managing, and using IT to accomplish NASA’s missions and programs. NPR 7120.5C,⁵ “NASA Program and Project Management Processes and Requirements,” March 22, 2005, defines a project as a specific investment identified in a program plan having defined goals, objectives, requirements, and life-cycle costs. It also addresses updating plans and documents when new content is added.

NASA Not in Full Compliance with NIST Assessment and Accreditation Procedures

NASA did not fully comply with NIST requirements for accrediting the PIV card issuer. Specifically, NASA properly conducted an assessment of the PIV card issuer, found deficiencies, and developed a corrective action plan 11 months after the HSPD-12 implementation office was established and 4 months before the Agency was to begin issuing HSPD-12 compliant PIV cards. However, NASA did not monitor the corrective action plan to ensure that the deficiencies identified were corrected, as required by Federal guidance and the IATO letter, and did not initiate a timely reassessment to accredit the card issuer, as required by Federal guidance.

NASA’s Independent Program Assessment Office conducted the first assessment of the PIV card issuer in April and May of 2007. That initial assessment cost NASA approximately \$110,000 and identified 78 deficiencies—60 low risk and 18 medium risk (medium risk deficiencies included inadequate documentation supporting completed training, inadequate procedures for assessing applicants, and a lack of an accreditation letter for the PIV card issuer’s information infrastructure). In accordance with NIST SP 800-79, the AIMO developed a corrective action plan to resolve the deficiencies.

NIST SP 800-79-1 states that the DAA may issue an authorization to operate (ATO) for the card issuer if the assessment results show that the card issuer conformed with FIPS 201-1. The DAA can only grant an ATO to a card issuer if there are no limitations

⁵ NASA issued NPR 7120.7, “NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements,” November 3, 2008, and directed that NPR 7120.7 be used for non-space flight programs and projects.

or restrictions imposed on any of its facilities included in the accreditation boundary. The DAA may issue an IATO if the DAA considers the discrepancies found during the assessment to be significant but the card issuer can address the deficiencies in a timely manner and there is an overarching necessity to allow the card issuer to operate. The card issuer must document the deficiencies in a corrective action plan so it can correct them during the accreditation process. Based on the independent assessment report and the corrective action plan, the DAA issued the PIV card issuer a yearlong IATO on June 12, 2007.

Terms and conditions the DAA stipulated in the IATO accreditation letter were that the PIV card issuer should only operate if NASA rigorously monitored the reliability of the PIV card operations and submitted quarterly reports detailing the status of the deficiencies listed on the corrective action plan. The AIMO stated that the corrective action plan was not monitored because he felt that the assessment that identified the deficiencies was inadequate. Monitoring and reporting on the deficiencies is intended to ensure that the deficiencies receive the proper visibility, prioritization, and resources necessary to resolve the issues and avoid problems that could have an adverse impact on NASA's ability to achieve full PIV card issuer accreditation.

Terms and Conditions of IATO Were Not Followed. The AIMO did not monitor actions taken to correct reported deficiencies and did not provide updates on the status of deficiencies identified during the assessment to ensure they were corrected, as required by the IATO and NIST. When NASA did not initiate a timely reassessment to accredit the card issuer, as required by NIST, the Agency issued two consecutive extensions to the IATO.

NASA's PIV card issuer became operational in January 2008 while under an IATO. In March 2008, 9 months after the first IATO was granted, the AIMO, through the Independent Program Assessment Office, initiated a limited PIV card issuer assessment, which resulted in the DAA extending the IATO to October 1, 2008—the first extension of the IATO. During this extension, NIST issued SP 800-79-1, the update, in June 2008. This revised document provided the methodology for assessing and accrediting PIV card issuers and was effective immediately upon issuance. Citing the issuance of revised guidance, the HSPD-12 Project Director determined that NASA would initiate reassessment of the PIV card issuer under the revised policy. In October 2008, the certification agent for the card issuer was preparing a plan for reassessing the PIV card issuer. The agent planned to conduct the reassessment at each NASA location but acknowledged that availability of funding would dictate how many locations would be included in the reassessment. The AIMO and the certification agent stated that because NIST had issued the revised policy for assessing PIV card issuers, the prior assessment results would not be used in the reassessment. However, we compared NIST SP 800-79 to NIST SP 800-79-1 and found that the major categories of requirements NASA had been deficient in were still required under the revised policy. Even though NASA personnel had not adhered to the conditions stipulated in the previous IATO letters, the

DAA extended the IATO a third time until March 1, 2009 (second extension under the June 2008-revised NIST policy).

The initial assessment of the NASA PIV card issuer cost about \$110,000. As of November 2008, NASA officials could not provide the cost for reassessing the PIV card issuer under the June 2008 NIST requirements because the certification agent was in the process of developing the reassessment plan. Since the AIMO did not monitor the progress toward correcting the deficiencies identified on the initial corrective action plan, NASA could incur costs associated with re-identifying the same deficiencies reported during the prior assessment.

We interviewed NASA and contractor staff and reviewed the IATO and PIV card issuer supporting documentation to determine if NASA personnel complied with the IATO and NIST policy. We found that NASA personnel did not update the corrective action plan or operations plan to reflect the current state of the PIV card issuer and that numerous technical deficiencies had not been reported or resolved.

NASA could also incur additional costs if the reassessment for accreditation does not successfully meet Federal requirements. Federal policy states that an agency can receive three IATOs to operate its PIV card issuer—an initial IATO and two additional consecutive IATOs—but failure to correct deficiencies found in the PIV card issuer after the expiration of the second consecutive IATO must result in an issuance of a denial of authorization to operate (DATO). NASA's noncompliance with the terms and conditions of the IATO and with NIST SP 800-79-1 increases the risk that the PIV card issuer may not be deemed reliable or capable of ensuring it enrolled and issued PIV cards only to authorized applicants. NASA is currently under its third IATO extension (second extension under NIST SP 800-79-1). If NASA does not adequately correct the deficiencies found in the card issuer operation, the DAA would have to issue a DATO in accordance with Federal policy. A DATO would mean a cessation of operation for the PIV card issuer and the possibility that NASA could be required to reissue its PIV cards after the card issuer is accredited, which could result in NASA incurring costs to reissue all PIV cards issued by the PIV card issuer.

Initiation of Reassessment for Accreditation Was Not Timely. The IATO states that the PIV card issuer is not considered accredited during the IATO period. NASA officials did not seek to reassess the PIV card issuer until March 2008—9 months after the DAA granted the first IATO. The original assessment was conducted while NIST SP 800-79 (the original version) was in effect, and NIST SP 800-79 states that an IATO is a temporary authorization to operate under specific terms and conditions and reassessment for accreditation should be initiated within 3 months of the date of the IATO.

The PIV card issuer began issuing PIV cards before an independent assessment verified the reliability of the card issuer. HSPD-12 requires that the card issuer be accredited to ensure that PIV cards are issued from a reliable card issuer. As of January 9, 2009, NASA had issued 72,024 (98.5 percent of the badges it expected to issue) PIV cards from

a card issuer that had not been accredited. Therefore, NASA runs the risk that the new assessment could disclose significant deficiencies that could eventually lead to a DATO and could cause NASA to spend, at minimum, \$1 million if the Agency has to reissue PIV cards to its employees and contractors.

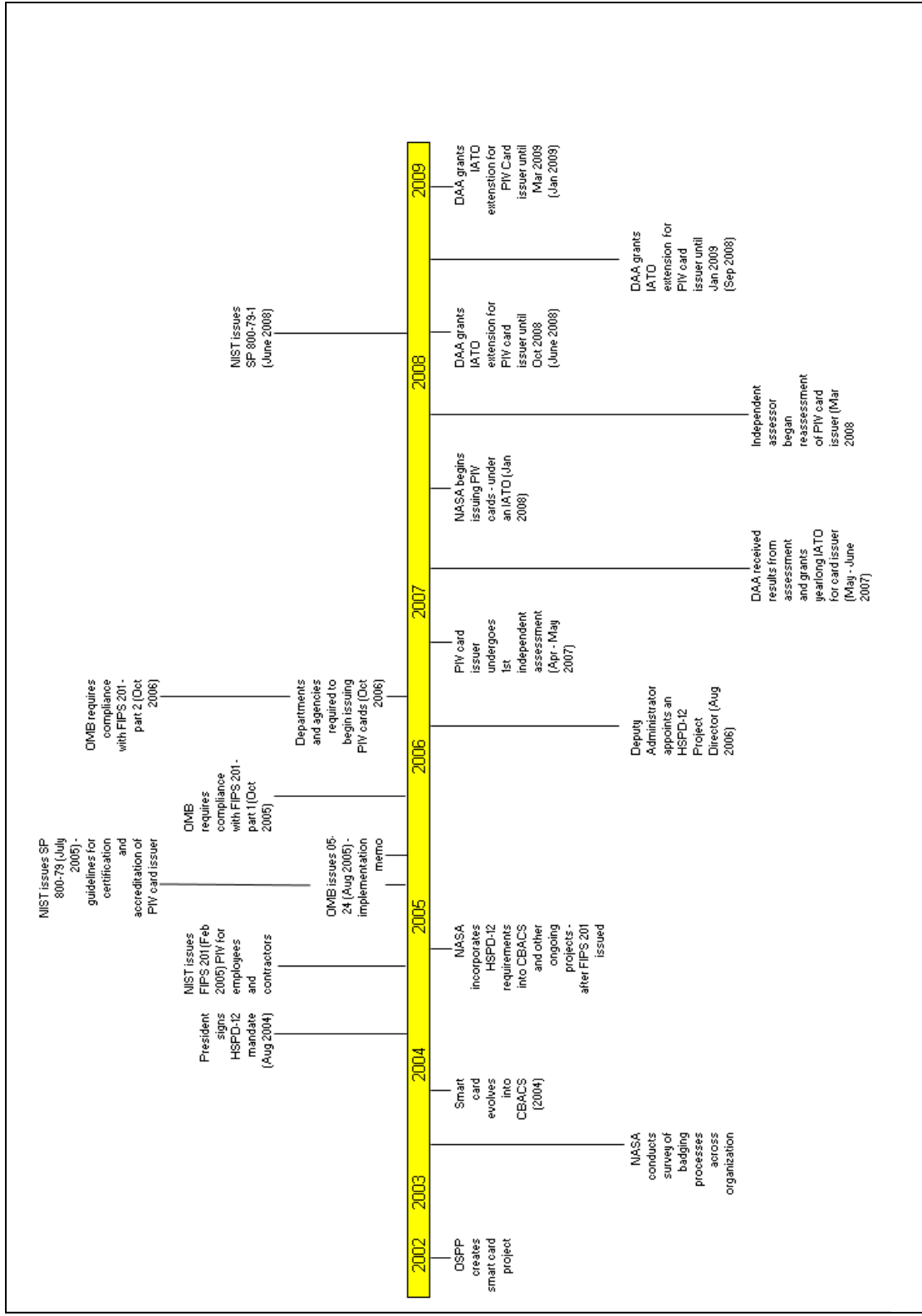
Noncompliance Caused by Lack of a Project Management Plan for HSPD-12 Implementation

HSPD-12 was signed in August 2004. However, NASA officials did not establish a project office with the authority to oversee HSPD-12 implementation for almost 2 years. In July 2006, NASA issued a memorandum establishing an Agency-level HSPD-12 project office responsible for identifying requirements and managing NASA's implementation of HSPD-12 requirements and appointed the HSPD-12 Project Director in August 2006. (See the Figure for a timeline of events.) The Project Director, who reported directly to the Deputy Administrator on a monthly basis and when requested, assembled a team consisting of HSPD-12 managers from each Center, appointed by each Center Director including Headquarters, and a member from each of the four main Mission Support Offices: Human Capital Management, Office of the CIO, OSPP, and Procurement.

Throughout the implementation processes, the Project Director expressed concerns about the lack of a project management plan to incorporate HSPD-12 and Federal requirements into ongoing projects, including CBACS. Those concerns, documented in monthly updates sent to the Deputy Administrator, noted the lack of

- a project management plan integrating the development projects that would be used to plan, execute, control changes, govern, monitor, and control the project;
- an integrated project schedule that would integrate the schedules of the subprojects and would further integrate the Center, program, and project implementation; and
- an integrated architecture that shows how all the pieces fit together technically and work flows for the process itself.

Figure. Timeline of NASA's implementation of PIV cards.



Despite the Project Director's concerns, NASA did not develop a project management plan; it was the AIMO's position that the PIV system was not a project but involved the implementation of several projects that were already in development. Thus, NASA managers continued to reference CBACS project management guidelines for developing subcomponents of the PIV system (developed before HSPD-12 was mandated) and did not update project-related documents to include HSPD-12 and FIPS requirements. However, NPR 7120.5C, addresses updating plans and documents when new content is added (e.g., the creation of a new project) and notes the need to evaluate modifications of the program plan due to changes in projects and activities within the program.

The HSPD-12 Project Director focused on meeting the OMB timelines and did not adhere to NASA's project management policy that required the Agency to update project plans. Thus, NASA focused its resources on implementing systems that would evolve into the PIV system. Within the first 2 months of being named HSPD-12 Project Director, the Director expressed concerns about the Agency's implementation approach, reporting to the Deputy Administrator that there was no integrated architecture to ensure that NASA personnel incorporated the Federal requirements into developing systems and that these issues could impact NASA's ability to meet the OMB deadline of October 2007.

Gap Analysis Not Conducted. Although the Project Director's position was that the PIV system involved implementing several projects already in development, NASA did not conduct or document a formal gap analysis to identify differences between those projects and FIPS 201-1 requirements. Gap analysis is defined as a technique for determining the steps to be taken in moving from a current state to a desired future-state. In IT systems, it begins with first identifying the system requirements of the present system(s) and comparing those requirements to requirements needed to achieve the desired results, thus highlighting the gaps in system requirements and identifying the components needed to achieve the desired end-state. NASA's project management policy had not required a formal gap analysis, however, NASA management has recognized the importance of identifying gaps between the systems NASA was using and those NASA was developing. In 2006, the NASA Deputy Administrator tasked program personnel to conduct a gap analysis on NASA's Integrated Enterprise Management Program to identify and characterize where management and business systems were not meeting the needs of the system users. However, HSPD-12 implementation personnel did not perform a gap analysis to identify differences between CBACS and other ongoing projects and HSPD-12 requirements; therefore, NASA had no formal means to demonstrate that its PIV system subcomponents would meet Federal requirements.

Recommendations, Management's Response, and Evaluation of Management's Response

Recommendation 1. The Assistant Administrator for the Office of Security and Program Protection should determine if the DAA for NASA's PIV card issuer should issue a DATO if subsequent reassessment results determine that significant deficiencies for PIV card issuer continue to exist.

Management's Response. On April 16, 2009, the Designated Approving Authority for NASA's PIV card issuer processes issued an authority to operate decision. As part of the decision, the Approving Authority directed the execution of a corrective action plan to address deficiencies noted during the PIV card issuer assessment.

Evaluation of Management's Response. The PIV card issuer was undergoing reassessment in March 2009 when we recommended that the DAA determine whether a DATO should be issued. Based on the reassessment results, the DAA issued an authorization to operate the PIV card issuer on April 16, 2009. Therefore, we consider the recommendation to be closed for reporting purposes.

Recommendation 2. The NASA Chief Information Officer and the Assistant Administrator for the Office of Security and Program Protection should follow Agency policy documented in NPR 2800.1 and NPR 7120.7 to plan and manage future development of IT projects.

Management's Response. The Office of the Chief Information Officer and the Office of Security and Program Protection concurred with the recommendation and stated that component projects that comprised the HSPD-12 were all planned and managed according to project management policy.

Evaluation of Management's Response. While NASA OCIO and OSPP concurred with the recommendation, the comments were not responsive. As discussed in the report, NASA had not updated ongoing project related documents to include HSPD-12 requirements. Management's response did not indicate how OCIO and OSPP plan to ensure that future IT development projects are planned and managed in accordance with NPR 2800.1 and NPR 7120.7. We consider the recommendation to be unresolved and request that the Assistant Administrator, Office of Security and Program Protection, and the NASA Chief Information Officer provide comments to this final report.

Recommendation 3. The NASA Chief Information Officer and the Assistant Administrator for the Office of Security and Program Protection should require system owners to conduct and document a gap analysis when Federal directives and requirements impact ongoing IT project development.

Management's Response. The Office of the Chief Information Officer and the Office of Security and Program Protection concurred with the recommendation and stated that a gap analysis of projects in development was conducted in the form of a business

architecture, which documented the overall framework and enabled detailed analysis of the as-is versus the to-be states.

Evaluation of Management’s Response. While OCIO and OSPP concurred with the recommendation, the comments were not responsive. The business architecture provided to OIG during the audit did show the “as is” and “to be” framework, but it did not show the gaps, in terms of the actual requirements and components, between what NASA was developing and what was needed to meet the HSPD-12 mandate. Management’s response did not indicate how OCIO and OSPP plan to ensure that system owners conduct and document a gap analysis when Federal directives and requirements impact ongoing IT development projects. We consider the recommendation to be unresolved and request that the OSPP Assistant Administrator and the NASA CIO provide comments to this final report.

FINDING B: LACK OF INTERNAL CONTROLS HAMPERED EFFECTIVE HSPD-12 IMPLEMENTATION

Although we did not identify any instances of PIV cards being issued to unauthorized individuals, NASA did not fully develop and employ sufficient internal controls to effectively implement HSPD-12 requirements. Specifically, the Agency did not ensure that NASA managers enforced PIV policies or procedures that required PIV personnel to receive training before performing assigned duties, or that NASA's policies were consistent for issuing temporary badges. These conditions occurred because personnel assigned PIV roles were unaware of the training requirement, and NASA had not developed and implemented policies for issuing temporary badges and HSPD-12 compliant PIV cards to non-NASA Federal employees. Also, NASA did not ensure that the PIV system provided a comprehensive audit trail to identify errors and irregularities. This condition occurred because NASA relied on audit capabilities in PIV system subcomponents instead of designing a single-audit capability to provide an audit trail for status requests in the PIV system. As a result of a lack of internal controls and inadequate system processes, the risk of issuing PIV cards to individuals who have not met security requirements or have no legitimate need to access NASA facilities or systems could be increased.

Federal and NASA Regulations

Federal agencies are responsible for developing and maintaining internal control activities that comply with OMB Circular A-123, "Management's Responsibility for Internal Control" (effective fiscal year 2006). NPD 1200.1E, "NASA Internal Control," July 21, 2008, provides NASA's internal control policy for complying with OMB Circular A-123.

FIPS 201-1 defines the PIV system Federal agencies are required to use to create common identification credentials, verify identity, and grant access to federally controlled facilities and information systems. The NASA Interim Directive (NID), "Personal Identity Verification (PIV) Policy and Procedures," May 24, 2007, implements FIPS 201-1 requirements and establishes NASA-wide policy for the creation and issuance of Federal credentials. NASA's process for issuing PIV cards involves having authorized personnel, using computerized systems, verify (1) an individual's identity has been authenticated (2) a background investigation was initiated, and (3) the individual is the intended recipient of the Federal credential.

FIPS 201-1 also requires that the PIV process include an audit trail that documents all actions taken for approving or denying requests for a PIV card. This audit trail is a critical component of the chain of trust for issuance and management of PIV cards.

Improved Internal Controls Needed for Training and Issuance of Temporary Badges

Training for PIV Personnel. Section 7 of the NID states that individuals designated for the roles require training and that for personnel involved in the PIV process, training will be provided. However, while the policy states that the individuals require training, it does not specifically state that the training must be completed prior to performing PIV duties; also, the training had not been added into the individuals' learning plan. We reviewed the training records of PIV personnel Agency-wide. We identified the total number of personnel assigned as PIV requestors, sponsors, and authorizers, as of August 12, 2008, to determine how many had completed the training. NASA policy states that individuals assigned a PIV role require training, which is provided through the online System for Administration, Training, and Educational Resources for NASA (SATERN). The following table details our findings:

Staff Completion of SATERN PIV Role Training^a			
PIV Role	Total	PIV Personnel	
		Completed SATERN Training	
		Number	Percentage
Requestor	1,236	401	32
Sponsor	842	250	30
Authorizer	77	30	39

^aTotal number of personnel by PIV role provided by a Project Manager for a PIV system subcomponent. Human Resources personnel provided SATERN training information.

Training records did not support that roughly 60 to 70 percent of personnel responsible for PIV card processing had completed the necessary training. The percentage of personnel completing the PIV role training was low because some PIV personnel completed training but the training records were not updated to reflect that they had completed the training, and PIV personnel we interviewed told us they were unaware the training was required. Inadequate training of PIV personnel could result in erroneous processing of PIV cards and issuing PIV cards to individuals who do not meet security requirements.

Issuing Badges. Conflicting policy statements and lack of guidance resulted in inconsistencies in how Centers issued badges. Specifically, NASA distributed a poster that outlined the configurations of temporary and permanent badges and stated that

temporary badges were effective for less than 180 days; however, NASA Centers issued temporary badges with 5-year expiration dates. For example, one Center issued 43 badges with 5-year expiration dates to Federal Aviation Administration and Army personnel detailed to NASA. According to the Center's HSPD-12 Implementation Manager, they were directed not to enroll and process non-NASA personnel for PIV cards because they were not employed with or through NASA. Therefore, that Center provided temporary badges with extended expiration dates. The NASA HSPD-12 Project Director supported the statement and added that NASA would not issue PIV cards to individuals from other Federal agencies. However, another Center had enrolled and issued PIV cards to 29 Department of Defense employees. The Center's Implementation Manager stated that there was no specific guidance prohibiting the Center from issuing PIV cards to non-NASA personnel. What guidance NASA did provide is in the NID, section 12.6, "Visitor and Temporary Badging," where it is noted that

Visitor and temporary badging is outside the scope of this document and is determined by each Center's security office, consistent with pertinent directives. Usually, a set of temporary visitor badges are held by the Badging Office and issued on an as-needed basis to authorized, temporary, and short-term visitors for appropriate access to NASA facilities. Short-term visitors will not receive access to protected logical data systems and resources. Individuals who require extensive physical or logical access, but for a period less than 6 months will be handled on a case-by-case basis in consultation with the Center Chief of Security. Access by visitor and temporary badges will be for bona fide purposes, and not used to circumvent the requirements of this Interim Directive.

Without specific guidance on the issuance and expiration of badges for non-NASA Federal Employees, NASA has no assurance that the Centers will use consistent methods for issuing badges. The lack of specific NASA guidance relating to issuing HSPD-12 compliant PIV cards to personnel from other Federal agencies allowed at least one NASA Center to disregard NASA's intent not to issue PIV cards to non-NASA Federal employees. Inconsistencies in badge issuance processes constitute noncompliance with NASA requirements.

Visibility of Data to Identify Errors and Irregularities

The PIV system did not provide sufficient data visibility to identify and explain possible errors or irregularities when processing PIV cards. An audit trail that details the status of PIV requests—including the names of personnel involved in processing the request, changes in the status of requests (e.g., change in employment status or personal data), and data relating to issuing, rejecting, or terminating access—should be readily available. FIPS 201-1, section A.2.3, requires that an audit trail documenting all actions be in place. The NASA PIV system did not include a readily available audit trail. For example, the system showed that PIV cards for some Headquarters contractor personnel had been requested, sponsored, and authorized. However, the PIV system inexplicably changed the status to show that the PIV cards had not been requested, sponsored, or authorized. Nevertheless, the PIV system showed that these contractor personnel had been enrolled

even though the system showed the PIV cards had not been requested or sponsored, which is a prerequisite to enrollment. NASA security personnel could not provide an explanation as to why these conditions occurred. Without a comprehensive audit trail, PIV personnel could overlook errors and irregularities when processing PIV cards. Unless deficiencies identified are corrected, NASA could increase the risk of issuing PIV cards to individuals who have no legitimate need to access NASA facilities or systems

PIV Card Maintenance Processes

NASA's focus so far has been on issuing PIV cards to all NASA and contractor employees rather than on maintaining the cards. However, PIV card maintenance must be integrated into department and agency procedures to ensure effective card management. PIV card maintenance includes the following processes:

- PIV card renewal is the process by which a PIV card is replaced without the cardholder having to repeat the full registration procedure.
- PIV card reissuance requires that the entire registration and issuance process, including fingerprint and facial image capture be repeated.
- Personal identification number reset occurs when the contents of the card are locked because the cardholder exceeded the number of attempts to access the system by typing an invalid identification number more than the allowed number of times stipulated by the Agency.
- PIV card termination occurs when the Agency permanently destroys or invalidates the card because the cardholder has separated (voluntarily or involuntarily) from Federal service, a contractor changes positions and no longer needs access to Federal buildings or automated systems, a cardholder is determined to be holding a fraudulent identity, or the PIV card itself is revoked.

The NID includes procedures for renewals, reissuances, personal identification number resets, and terminations of PIV cards.

Since the Agency has not yet focused on card maintenance, including terminations, we did not evaluate the adequacy of those efforts. However, we noted a potential area of vulnerability in the PIV card termination process that may become significant. Specifically, there might be a risk to NASA's automated systems if contractor employees fail to surrender their PIV cards prior to departure from NASA and, thus, retain access to NASA facilities and systems. Once the cards have the technical capability to provide not only physical access to NASA facilities but also logical access to NASA computer systems, the risk of PIV card misuse greatly increases. OIG may evaluate this vulnerability at a later date when the PIV cards have logical access capability.

Recommendations, Management's Response, and Evaluation of Management's Response

Recommendation 4. The Assistant Administrator for the Office of Security and Program Protection should notify all personnel involved in the PIV process of the requirement to complete the required training prior to performing their PIV duties and add the training requirement to the individuals' SATERN learning plan.

Management's Response. OSPP concurred but stated that the Agency Identity Management Official (AIMO) had posted training for the various roles in the PIV card issuance process on OSPP's Web site, and individuals performing those roles were directed to take that training. Once training was installed in SATERN, individuals were directed to SATERN so that training was recorded. However, individuals who had taken the training via OSPP's Web site had not received credit in SATERN. OSPP noted that the AIMO will work with appropriate officials to ensure that the OSPP Web site trained individuals take training via SATERN and that the training becomes part of each of their learning plans as well as part of the training plan for anyone who has a role in the PIV card issuance process. OSPP stated it will update OIG one year from April 20, 2009, or when the items have been addressed and completed.

Evaluation of Management's Response. OSPP's actions are responsive, and the recommendation is resolved but will remain open for reporting purposes until all corrective actions have been completed and we have verified completion of those actions.

Recommendation 5. The Assistant Administrator for the Office of Security and Program Protection should develop and implement NASA policies for issuing temporary badges and HSPD-12 compliant PIV cards to individuals assigned to NASA locations from other Federal agencies and establish and include appropriate expiration date guidelines in the NASA policy for temporary badges.

Management's Response. OSPP concurred, stating that the AIMO had taken steps to implement procedures for issuance of temporary-workforce badging and limit their use to no more than 179 consecutive days. OSPP stated it will update the OIG one year from April 20, 2009, or when the items have been addressed and completed.

Evaluation of Management's Response. OSPP's actions are responsive, and the recommendation is resolved but will remain open for reporting purposes until all corrective actions have been completed and we have verified completion of those actions.

Recommendation 6. The Assistant Administrator for the Office of Security and Program Protection should modify the PIV system to increase data visibility by modifying the system and incorporating a single-audit infrastructure that pulls the necessary audit trail data from the PIV system subcomponents.

Management's Response. OSPP concurred, stating that a central audit database has been configured and auditable information was being transitioned into a new structure. OSPP stated it will update OIG one year from April 20, 2009, or when the items have been addressed and completed.

Evaluation of Management's Response. OSPP's actions are responsive, and the recommendation is resolved but will remain open for reporting purposes until all corrective actions have been completed and we have verified completion of those actions.

FINDING C: NASA RESPONDS TO ISSUES RELATED TO ROLE SEPARATIONS

NASA did not ensure that PIV system operations included proper separation of roles and duties. The Assistant Administrator for OSPP assigned the same individual to perform both the AIMO and DAA responsibilities because of staffing issues. By assigning one person to fulfill AIMO and DAA roles, NASA risked the integrity of its assessment and accreditation process and ultimately could put the reliability of the NASA PIV card issuer in question. In addition, the PIV system did not prevent the same individual from performing the duties of both the PIV card sponsor and authorizer. NASA increased the risk of issuing a PIV card to unauthorized individuals by allowing one person to sponsor and authorize an applicant's PIV card request.

Federal and NASA Guidance on Separation of PIV Oversight and Staffing Roles

SP 800-79-1 defines the DAA as “an official of the organization with the authority to review all assessments of a PIV card issuer and its facilities, and to accredit the PIV card issuer as required by HSPD-12.” Through accreditation, the DAA accepts responsibility for the operation of the PIV card issuer at an acceptable level of risk to the organization.” SP 800-79-1 defines the OIMO (AIMO at NASA) as being “responsible for implementing policies of the organization, assuring that all specified procedures of the PIV card issuer are being performed reliably, and providing guidance and assistance to the PIV card issuer Facilities.” It further states that the OIMO cannot fulfill the role of the DAA.

Similarly, FIPS 201-1, section 2.2, requires that the PIV process adhere to the principle of separation of duties assigned to agency PIV personnel to ensure that the same individual cannot issue a PIV card without the cooperation of another authorized person. In addition, the NID states that an individual cannot be both sponsor and authorizer for processing the PIV card of a given applicant.

Dual Assignment Compromised Process Integrity

NASA assigned the same individual to perform responsibilities of both AIMO and DAA. In February 2007, the Senior Agency Official for HSPD-12 implementation assigned the Deputy Assistant Administrator for OSPP as DAA and another OSPP official as AIMO. However, in June 2008 when the Deputy Assistant Administrator left NASA, the Interim

Assistant Administrator for OSPP reassigned the DAA role to the individual already assigned the AIMO role.

NASA personnel told us that their interpretation of the Federal policies and the lack of HSPD-12 knowledgeable personnel resulted in the noncompliance. OSPP officials stated that NIST SP 800-79-1 contradicted itself. OSPP officials referred to NIST SP 800-79-1, section 2.6.7, which states that while roles are independent and should be filled by different people, there may be a need to have one person fill more than one role. However, NIST SP 800-79-1, section 2.6.3, clearly states that the OIMO/AIMO cannot fulfill the role of the DAA. OSPP officials stated that another reason for appointing one person to both positions was staff turnover in OSPP. The office had limited personnel who were knowledgeable about the assessment and accreditation required to comply with the HSPD-12 mandate. As a result, the Interim Assistant Administrator for OSPP assigned the DAA role to the individual already performing the AIMO role for NASA.

NIST's assessment and accreditation processes for the card issuer assign AIMO and DAA responsibilities to two different individuals to ensure (1) an independent determination of the decision to operate the card issuer; (2) effective control activities for the Agency's planning, implementing, reviewing, and accountability for Government resources; and (3) achievement of effective results. The results of an assessment are presented to the AIMO who reviews the assessment findings and prepares recommended corrective actions. By assigning the AIMO and DAA roles to the same person, OSPP effectively eliminated a part of NASA's oversight chain of command for the PIV card issuer, thus jeopardizing the integrity of the Agency's assessment and accreditation process.

On January 12, 2009, the Senior Agency Official for HSPD-12 issued a letter assigning the responsibilities of the DAA to the interim Deputy Assistant Administrator, OSPP -the interim Deputy Assistant Administrator was assigned to the position on January 4, 2009. Therefore, we did not include a recommendation to assign two different individuals the responsibilities for performing the AIMO and the DAA functions.

Staffers Acting as Both Sponsor and Approver Identified Inadequate Process Controls

NASA did not have sufficient separation of duties among personnel responsible for processing PIV cards. Specifically, controls were inadequate to prevent an individual from assuming the roles of both sponsor and authorizer when processing an applicant's PIV card request. The process did include a control in the form of a computer query to compare the identity of the sponsor against that of the authorizer for each PIV card request. However, this was a manual process—i.e., the PIV system did not automatically perform the query; it required PIV personnel to initiate the query. If the same individual was both sponsor and authorizer, personnel at Marshall were supposed to reject the

request before ordering the PIV card. Because this control was not automated, there was no assurance that PIV personnel performed the computer query.

PIV staffing roles responsible for issuance of PIV cards have the same need for separation of duties to prevent one individual from assuming the roles of both sponsor and authorizer when processing an applicant's PIV card request. PIV roles are as follows:

- PIV requester creates an initial request for a PIV card for an applicant (civil service or contractor employee).
- PIV sponsor, a Federal employee, approves the need for the PIV card.
- PIV enrollment official collects, establishes, and verifies identity using the applicants' Federal and state picture identification and fingerprints.
- PIV authorizer, a Federal employee in the Center's security office, adjudicates the results of the applicant's background investigation and authorizes the production and issuance of the PIV card.
- PIV issuance official issues the PIV card to the applicant upon reverification of the applicant's identity.

We found that personnel at two Centers did not process PIV card requests according to policy. Specifically, at one Center, the same individual sponsored and authorized 14 PIV card requests; at another Center, the same individual sponsored and authorized 29 PIV card requests. Having one person act as both sponsor and authorizer when processing an applicant's PIV card request violates Federal and NASA policy and increases the risk of issuing PIV cards to individuals who have no legitimate need to access NASA facilities or automated systems. After we brought this to management's attention, as directed by personnel at Marshall, both Centers reprocessed those PIV card requests to comply with the separation of duties requirement. In addition, PIV officials upgraded the PIV system adding controls to prevent one individual from performing conflicting PIV duties. Therefore, we are not making a recommendation regarding separation of duties.

Scope and Methodology

We performed this audit from January 2008 through February 2009 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 believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Since we performed the audit during NASA's PIV card issuance phase of HSPD-12 implementation, we focused our work on the Agency's process for issuing PIV cards. We did not perform audit work on NASA's process for maintaining PIV cards because the Agency's processes were not mature enough.

We performed the following audit procedures:

- reviewed Federal and NASA guidance including HSPD-12, FIPS 201-1; NIST SP 800-79; NIST SP 800-79-1; NPD 1200.1E; NPD 2800.1; NPD 2800.1A; NPD 2800.1B; NPR 2800.1; and NPR 1600.1, which included the NID for PIV policies and procedures;
- interviewed key NASA personnel including the Agency HSPD-12 Implementation Manager, HSPD-12 technical personnel at Marshall, and Center security officials responsible for the PIV card process at NASA Headquarters, Ames Research Center (Ames), and Johnson Space Center (Johnson), to understand NASA's approach for complying with HSPD-12;
- reviewed the adequacy of the assessment and accreditation of the PIV card issuer;
- conducted an initial survey of the PIV card process at Headquarters, Ames, and Johnson;
- observed processing of PIV cards at Headquarters, Ames, and Johnson;
- evaluated the PIV system controls through interviews with and demonstrations provided by Marshall's HSPD-12 technical personnel;
- issued a questionnaire to all Center security officials to obtain information about the Centers' practices for issuing temporary identification cards to newly hired employees, reissuing PIV cards to replace lost or expired ones, and collecting and terminating the PIV cards of departed employees;
- determined whether the PIV system provides sufficient data visibility needed by personnel to properly process PIV cards; and

- selected statistical samples of PIV cards issued to recently hired personnel at each NASA Center and determined whether the Centers' processed PIV cards in accordance with Federal and NASA policies.

Use of Computer-Processed Data. We used listings generated by the PIV system to select samples of issued, reissued, and terminated PIV cards for review. To assess the accuracy and completeness of those listings, we compared them to other listings (e.g., from human resource organizations) generated outside of the PIV system. We found inconsistencies among the listings but determined that they have minimal impact on the integrity of our sample selection process.

Review of Internal Controls

We determined whether the PIV system contains built-in system controls to ensure the processing of PIV cards is in accordance with Federal laws and NASA policies. We also reviewed the PIV process to ensure proper separation of duties among personnel responsible for processing PIV cards. Overall, controls were adequate. However, as reported in the third finding, we noted a minor deficiency regarding the PIV system's ability to ensure separation of duties for the PIV sponsor and PIV authorizer roles, which NASA took actions to correct during the audit.

Prior Coverage

During the last 5 years, the Government Accountability Office (GAO) issued two reports of particular relevance to the subject of this report. Unrestricted reports can be accessed over the Internet at <http://www.gao.gov>.

“Additional OMB Leadership Needed to Optimize Use of New Federal Employee Identification Cards” (GAO-08-292, February 2008).

“Agencies Face Challenges in Implementing New Federal Employee Identification Standard” (GAO-06-178, February 2006).

MANAGEMENT COMMENTS

National Aeronautics and Space Administration
Headquarters
Washington, DC 20546-0001



April 20, 2009

Reply to Attn of:

Office of Security and Program Protection

TO: Assistant Inspector General for Auditing

FROM: Assistant Administrator, Office of Security and Program Protection

SUBJECT: Consolidated Response to: Draft Audit Report, "NASA's Processes for Providing Personal Identity Verification (PIV) Cards Were Not Completely Effective in Meeting Federal Requirements" (Assignment No. A-08-009-00)

Reference: Assistant Inspector General for Auditing memorandum dated March 20, 2009

The Office of Security and Program Protection (OSPP) and the Office of the Chief Information Officer (OCIO) have reviewed the subject report and herein are providing a consolidated response as requested.

NASA has issued nearly 75,000 PIV credentials to its workforce. The Senior Agency Official (SAO) for the PIV Card Issuance (PCI) process does not deem the issues identified in either the OIG report, or the PCI Assessment report to pose such risks that would require reissuance of these credentials. As stated in the OIG report, "... We did not identify any instances of PIV cards being issued to unauthorized individuals..." Therefore, the SAO does not concur with the OIG's assessment that NASA may need to reissue credentials.

The SAO and OCIO have reviewed OIG's recommendations and the feedback to them is as follows:

Recommendation (1): Determine if the designated accreditation authority for the PIV card issuer should issue a denial of authorization to operate if subsequent reassessment results determine that significant deficiencies for the PIV card issuer continue to exist.

OSPP/OCIO comments: On April 16, 2009, the Designated Approving Authority (DAA) for NASA's PCI processes issued an Authority To Operate (ATO) decision to the Agency Identity Management Official (AIMO). As part of the ATO, the DAA directed the execution of a Corrective Action Plan (CAP) to address deficiencies noted during the PCI Certification and Accreditation (C&A) review conducted by the Assessor as directed by the National Institutes of Standards and Technology (NIST) Special Publication 800-79-1 (NIST SP 800-79-1). Without significant changes to the PCI processes, the ATO is scheduled to expire on April 16, 2012.

Recommendation (2): Follow Agency procedural requirements to plan and manage future development of information technology (IT) projects.

OSPP/OCIO comments: OSPP/OCIO concurs. The component projects that comprised the overall HSPD-12 infrastructure were all planned and managed according to NPR 2800.1 and NPR 7210.5 (the predecessor to 7120.7 which was not published until 11/03/2008).

Recommendation (3): Require system owners to conduct and document a gap analysis when Federal directive and requirements impact ongoing IT project development.

OSPP/OCIO comments: OSPP/OCIO concurs. A gap analysis of the existing projects in development was conducted in the form of the HSPD-12 Business Architecture, which documented the overall framework for the business of identity, credential and access management down to the processes and business rules and enabled detailed analysis of the as-is vs. the to-be states. This business architecture has been made widely available and has been of great interest in various identity related Federal forums.

Recommendation (4): Notify all personnel involved in the PIV process of the requirement to complete training prior to performing their PIV duties and add the training requirement to the individuals' NASA learning plan.

OSPP/OCIO comments: OSPP/OCIO concurs. Until such time as training could be placed into the System for Administration, Training and Educational Resources for NASA (SATERN), the Agency Identity Management Official (AIMO) posted training for the various roles within the Personal Identity Verification (PIV) Credential Issuance (PCI) process on the OSPP web site. Individuals performing PCI roles were directed to take the training via the web site. Once training had been installed within SATERN, individuals who had taken the training via the web site were grand fathered, however, appropriate credit was not notated in SATERN. All other individuals were directed to the SATERN so that training was recorded. The AIMO will work with appropriate officials to ensure that grand fathered individuals take training via SATERN, and that PCI training become part of each of their learning plans, and part of each individual's training plan that has a role in the PCI process.

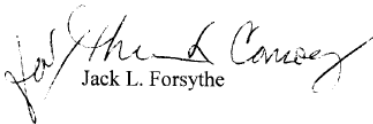
Recommendation (5): Develop and implement NASA policies for issuing temporary badges and HSPD-12 compliant PIV cards to non-NASA Federal employees assigned to NASA locations and establish and include appropriate expiration date guidelines for temporary badges.

OSPP/OCIO comments: OSPP/OCIO concurs. The AIMO has taken steps to implement temporary-workforce badging procedures that will retire the previously used topology and limit issuance to no more than 179 consecutive days.

Recommendation (6): Modify the PIV system to increase data visibility by modifying the system and incorporating a single-audit infrastructure that pull the necessary audit trail data from the PIV system subcomponents.

OSPP/OCIO comments: OSPP/OCIO concurs. The NASA PIV Team was able to provide the OIG auditors all of the information requested. However, we do agree that a central repository would be beneficial to the auditing and tracking of the system. At this time, a central audit database has been configured and migration of auditable information is being transitioned into this new structure.

OSPP will provide an update to the OIG one-year from the date of this memorandum, or when all items have been addressed and completed. OSPP point of contact for this matter is the Agency Identity Management Official, Theresa Conroy. Ms. Conroy can be reached at terry.conroy@nasa.gov, or 202-358-5183.


Jack L. Forsythe

cc:
OCIO/Mr. Hecker
OCIO/Ms. Petraska
OCIO/Ms. Irwin
OSPP/Ms. Conroy
OSPP/Dr. Martin

REPORT DISTRIBUTION

National Aeronautics and Space Administration

Administrator
Deputy Administrator
Chief of Staff
Chief Information Officer
Assistant Administrator, Office of Security and Program Protection

Non-NASA Organizations and Individuals

Office of Management and Budget
Deputy Associate Director, Energy and Science Division
Branch Chief, Science and Space Programs Branch
Government Accountability Office
Director, Defense, State, and NASA Financial Management, Office of Financial Management and Assurance
Director, NASA Issues, Office of Acquisition and Sourcing Management

Congressional Committees and Subcommittees, Chairman and Ranking Member

Senate Committee on Appropriations
Subcommittee on Commerce, Justice, Science, and Related Agencies
Senate Committee on Commerce, Science, and Transportation
Subcommittee on Space, Aeronautics, and Related Sciences
Senate Committee on Homeland Security and Governmental Affairs
House Committee on Appropriations
Subcommittee on Commerce, Justice, Science, and Related Agencies
House Committee on Oversight and Government Reform
Subcommittee on Government Management, Organization, and Procurement
House Committee on Science and Technology
Subcommittee on Investigations and Oversight
Subcommittee on Space and Aeronautics

Major Contributors to the Report:

Wen Song, Director, Information Technology Directorate

Denise Saenz, Project Manager

Mario Carbone, Project Manager

Bessie Cox, Team Lead

Howard Kwok, Auditor

Bret Skalsky, Auditor

Chris Reeves, Technical Specialist

Janet Overton, Editor



OFFICE OF AUDITS

OFFICE OF INSPECTOR GENERAL

ADDITIONAL COPIES

Visit <http://oig.nasa.gov/audits/reports/FY09> to obtain additional copies of this report, or contact the Assistant Inspector General for Auditing at 202-358-1232.

COMMENTS ON THIS REPORT

In order to help us improve the quality of our products, if you wish to comment on the quality or usefulness of this report, please send your comments to Ms. Jacqueline White, Quality Assurance Division Director, at Jacqueline.White@nasa.gov or call 202-358-0203.

SUGGESTIONS FOR FUTURE AUDITS

To suggest ideas for or to request future audits, contact the Assistant Inspector General for Auditing. Ideas and requests can also be mailed to:

Assistant Inspector General for Auditing
NASA Headquarters
Washington, DC 20546-0001

NASA HOTLINE

To report fraud, waste, abuse, or mismanagement, contact the NASA OIG Hotline at 800-424-9183 or 800-535-8134 (TDD). You may also write to the NASA Inspector General, P.O. Box 23089, L'Enfant Plaza Station, Washington, DC 20026, or use <http://oig.nasa.gov/hotline.html#form>. The identity of each writer and caller can be kept confidential, upon request, to the extent permitted by law.