

**SBA'S IMPLEMENTATION OF AN HSPD-12
CARD ISSUANCE SYSTEM**

Report Number: 09-01

Date Issued: October 6, 2008

**Prepared by the
Office of Inspector General
U. S. Small Business Administration**



Office Inspector General

Memorandum

To: Robert F. Danbeck
Associate Administrator for Management
and Administration

Date: October 6, 2008

Christine Liu
Chief Information Officer
/s/ Original Signed

From: Debra S. Ritt
Assistant Inspector General for Auditing

Subject: Final Report on SBA's Implementation of an HSPD-12 Card Issuance System
Report No. 09-01

This report addresses SBA's effort to develop and implement a system for issuing Personal Identity Verification (PIV) cards in accordance with Homeland Security Presidential Directive 12 (HSPD-12). Due to wide variations in the quality and security of the forms of identification used to access Federal facilities, HSPD-12 required agencies to issue secure and reliable identification cards to their employees and contractors. Our audit objectives were to assess SBA's: (1) progress in meeting requirements established by the Office of Management and Budget (OMB) and the National Institute of Standards (NIST) for developing a card issuance system; and (2) compliance with Agency policies governing systems development projects.

To assess the Agency's progress in developing a card issuance system, we reviewed project plans for SBA's HSPD-12 card issuance system, called the *Identity Management System (IDMS)*, Agency budget submissions, and project reports sent to OMB. We compared reported contract deliverables and implementation dates for key activities with HSPD-12 implementation requirements. These requirements are outlined in OMB Memorandum 05-24, *Implementation of HSPD-12 Policy for a Common Identification Standard for Federal Employees and Contractors*, and Federal Information Processing Standards (FIPS) Publication 201-1, *Personal Identity Verification of Federal Employees and Contractors*, issued by NIST. We also evaluated SBA's compliance with criteria for assessing agency capability to perform the required card issuance services contained in NIST Special Publication (SP) 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*

and SP 800-79-1, *Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations*.

We reviewed SBA guidelines and standards for systems development contained in its *Systems Development Methodology (SDM)* and compared them to actions taken by the project team in developing IDMS. The audit was conducted between November 8, 2007 and September 2, 2008 in accordance with *Government Auditing Standards* prescribed by the Comptroller General of the United States.

BACKGROUND

On August 27, 2004, the President of the United States signed HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*. This directive mandated a secure and reliable form of identification for Federal employees and contractors. Secure and reliable forms of identification are those that meet the security and control objectives of HSPD-12 by being: (1) issued based on sound criteria for verifying an individual's identity; (2) strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (3) able to be rapidly authenticated electronically; and (4) issued only by providers whose reliability has been established by an official accreditation process.

To address the control and security objectives of HSPD-12, in February 2005, NIST issued FIPS 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, which established the minimum requirements for card issuing agencies and for developing a Federal PIV system. The publication describes the card elements, system interfaces and security controls required to securely store, process, and retrieve identity credentials from the card. The standards consist of two parts—PIV-I, which addresses the control objectives and security requirements of HSPD-12, and PIV-II, which addresses the technical interoperability requirements of the directive.

To implement HSPD-12, on August 5, 2005, OMB issued Memorandum 05-24, *Implementation of HSPD-12 Policy for a Common Identification Standard for Federal Employees and Contractors*, requiring Federal departments and agencies to:

- Adopt and accredit an identity proofing, registration, and card issuance process for employees and contractors, consistent with the security and control objectives of HSPD-12 (i.e., become PIV-I compliant) by October 27, 2005;
- Begin deploying products and a card issuance system that meet the requirements of HSPD-12, and begin requiring identity credentials for

facility access. This also included establishing the minimum requirements of a PIV card that allows interoperability for physical and logical access (i.e., become PIV-II compliant) by October 27, 2006;

- Verify and/or complete background investigations and issue PIV cards for all employees with less than 15 years of service and all contractors by October 27, 2007; and
- Verify and/or complete background investigations and issue PIV cards for all employees with more than 15 years of service by October 27, 2008.

In 2005, SBA budgeted \$4.9 million through Fiscal Year 2008 to develop and deploy IDMS, and to produce 4,500 PIV cards. The entire \$4.9 million was to be financed out of operating funds. In an October 2006 Federal Register Notice, SBA announced it had deployed IDMS. To date, SBA has spent \$3.3 million of the \$4.9 million budgeted for the HSPD-12 initiative on the acquisition of hardware and software, as well as integration and project management services. As of June 30, 2008, SBA had issued 379 of the 4,500 identity cards needed for its employees, but no cards to any of its contractors.

RESULTS IN BRIEF

SBA has not fully satisfied any of the three OMB requirements that were to be implemented by October 2007, and will not meet a fourth set for October 2008. SBA has not been certified or accredited as an organization capable of developing and operating an HSPD-12 compliant card issuance system; did not ensure that the development contractors were GSA-approved; and did not perform a security review of IDMS to ensure that the privacy data it maintains is adequately protected. More specifically:

- The Agency established an identity proofing and registration process and designed IDMS by the October 2005 deadline. However, IDMS is not PIV-I compliant. SBA has not undergone a Certification and Accreditation (C&A) review of its organization to establish that it has the capability, personnel, equipment, finances, and support infrastructure needed to develop and operate the system, as required by NIST guidelines.
- SBA deployed IDMS by the OMB deadline of October 2006. However, the Agency did not perform a security C&A review of the system to demonstrate that the system is secure and reliable to satisfy the control and security objectives of HSPD-12. The technical interoperability of IDMS has also not been tested to determine whether it is PIV-II compliant. In addition, SBA has not ensured that the development contractors it used were General Services Administration (GSA)-

approved and has not certified that the contractor's products and services adhere to the Federal standards set forth for the HSPD-12 initiative.

- Only 379 of the 4,500 PIV cards needed for SBA's employees have been issued, and none had been issued to SBA's 312 contractors as of June 30, 2008. Presently, SBA presently does not track the issuance of PIV cards based on employees' years of service and we were unable to determine how many employees with less than 15 years of service should have been issued identity cards by the October 27, 2007 deadline.

SBA is also not on schedule to meet the fourth requirement—the issuance of identification cards for all employees with more than 15 years of service—which must be implemented by October 27, 2008. Currently, the Agency estimates that this requirement will not be completed until December 31, 2009, or 15 months after the required implementation date.

Moreover, in building IDMS, SBA did not fully comply with its own SDM policy to ensure that the project met the Agency's standards for security, integrity, and availability. For example, SBA did not ensure that HSPD-12 requirements were incorporated into the IDMS design specifications and did not complete fundamental project planning and management documents needed to ensure that the system was properly designed and tested to ensure that it functioned as intended. SBA also did not follow systems development protocol or conduct acceptance testing when introducing major software and hardware changes. Consequently, since IDMS was deployed, it has experienced server freezes, data integrity issues, user processing bottlenecks, and problems capturing and verifying fingerprints, among other issues. For example, a February 2008 software modification rendered the display of employee photos on the IV card unreadable by the new system.

SBA also did not follow its own capital investment policy, which is prescribed by the SDM, to ensure that IDMS was managed within budget and schedule or complied with OMB requirements for project funding. According to the Agency's *Capital Planning Investment Control* procedures, major IT investments costing more than \$200,000 in a single year or more than \$500,000 in 3 years must use Earned Value Management techniques to manage project cost, schedule and technical performance. OMB also requires that major IT investments be approved as capital projects through the OMB Exhibit 300 process. Under this process, the Agency reports to OMB a baseline plan for accomplishment of the project's cost, schedule and technical objectives. However, despite these requirements, SBA neither used an Earned Value Management system nor treated IDMS as a capital project. Instead, IDMS was funded out of the Agency's operating budget. Consequently, it cannot be determined whether project expenditures were appropriate according to the

project schedule and actual work completed, or whether additional funding is needed to meet performance objectives.

Based on the significant risk of maintaining PIV data on a system that has not undergone the required security reviews, we recommended that SBA immediately cease IDMS operations until the system is deemed capable of protecting the privacy data it contains. We also believe this to be a security weakness reportable under the Federal Information Security Management Act (FISMA), requiring monitoring through the Agency's security remediation process, and plan to report it, accordingly.

We also recommended that SBA implement the provisions of NIST 800-79-1 and FIPS 201-1 by securing a C&A of the Agency as a PIV Card Issuing Organization; an accreditation of all HSPD-12 products and services provided by third parties; and a security C&A of IDMS. SBA should also conduct acceptance tests to ensure that IDMS meets functional requirements, including reading and authenticating the digital certificates on PIV cards. Finally, because it is unclear how much additional investment in IDMS will be required to correct performance and security problems, and the project is a major IT investment, SBA should use Earned Value Management techniques to manage project performance and report to OMB, through the Exhibit 300 process, a baseline plan for accomplishment of the project's objectives.

In written comments on a draft of this report, SBA took issue with the characterization of its progress in implementing the HSPD-12 initiative, stating that although it provided a number of documents to the OIG as evidence of its compliance with OMB guidance on this initiative, the documentation did not receive a thorough review prior to the draft being issued. We disagree with SBA's assertion. The documentation that SBA provided during the audit did not demonstrate that SBA had undergone a C&A review of its organization; performed a security C&A of IDMS to demonstrate that the system is secure and reliable, or followed its own requirements to use earned value management in planning and managing the IDMS project. The OIG made repeated attempts to obtain support for the Agency's assertions, but the OCIO was unable to produce evidence of its compliance, and in its response to this report, acknowledged that it had not completed a C&A of IDMS.

Management also concurred with two of the five recommendations, partially disagreed with one, and disagreed with two. A detailed discussion of the comments begins in the "Agency Comments" section of this report, and the comments in their entirety are included in Appendix I.

RESULTS

SBA Met Two Project Deadlines, but Did Not Fully Satisfy OMB and NIST Requirements for Developing a Secure and Reliable System

To date, SBA reported that it met two key milestones established for 2005 and 2006—the implementation of an identity proofing, registration and card issuance process by October 2005, and deployment of IDMS by October 2006. Although the first two deadlines were met, the audit determined that SBA did not fully satisfy the OMB and NIST requirements associated with these deadlines.

Further, SBA has not fully complied with the requirements for the third deadline and is not on schedule to meet the fourth. Although PIV cards were required to be issued to all employees with less than 15 years of service by October 27, 2007, as of June 30, 2008, SBA had issued only 379 employee cards and no cards to the 312 contractors on board at that time. Because SBA has not determined the number of employees that have less than 15 years of service, we could not determine the number of employee cards that SBA should have issued by the October 2007 deadline. According to SBA, it will also not meet the October 2008 deadline for issuing cards to its employees with more than 15 years of service. This milestone is not expected to be met until December 2009—15 months after the required date.

SBA Did Not Fully Satisfy the Requirements of the First Milestone

FIPS 201-1 requires that to be PIV-I compliant all card issuing agencies must undergo a C&A review by an independent third-party prior to issuing PIV cards. This review assesses the capabilities and reliability of the Agency to perform the required card issuance services required by HSPD-12. The criteria for evaluating an agency's capabilities are outlined in NIST SP 800-79-1, *Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations*. Although the C&A review was one of the four major requirements of HSPD-12, SBA had not complied with this requirement by the October 2005 deadline.

Further, as of August 22, 2008, SBA was still not certified or accredited as an organization capable of developing and operating an HSPD-12 compliant card issuance system. Although SBA had prepared an Operations Plan and other documents required for the C&A review, it had not completed the accreditation package or obtained the required approvals of the package needed for the C&A assessment of its HSPD-12 operations.

On June 30, 2008, NIST issued an update of SP 800-79, emphasizing the importance of determining whether card issuing organizations are capable of performing the card issuance services required of HSPD-12. This guidance further states that card issuing organizations should issue PIV cards only after

they have been authorized to operate based on the assessment criteria outlined in SP 800-79-1. More importantly, the publication stresses that agencies that have started issuing PIV cards, but which do not meet the accreditation guidance, should immediately halt card issuance operations. Finally, the guidance states that the accreditation of a card issuing organization requires prior accreditation of the security of all information used by the agency in accordance with SP-800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*.

Because SBA started issuing PIV cards without securing a C&A of its card issuance operations and also lacks prior accreditation of the security of all of its related information systems, it should immediately cease IDMS operations, as required by the June 2008 NIST guidance. We believe this constitutes a security weakness reportable under FISMA that should be monitored through the Agency's security remediation process. Accordingly, we plan to report the issue as a security deficiency in our FISMA review.

Finally, SBA has not complied with the requirement that all HSPD-12 products and services provided by third parties undergo an accreditation review by October 2005 to ensure that they conform to Federal standards. OMB M-05-24 informed agencies that all HSPD-12 products and services must be approved by GSA and be included on GSA's *Approved Products List*. Any agency making procurements outside of GSA vehicles for approved products and services must certify that "...the products and services procured meet all applicable Federal standards and requirements, ensure interoperability and conformance to applicable Federal standards for the lifecycle of the components, and maintain a written plan for ensuring ongoing conformance to applicable Federal standards for the lifecycle of the components."

SBA's contractor, who was responsible for the IDMS systems integration, was not on GSA's approved list. SBA also did not certify that the contractor's products and services adhered to Federal standards; ensure interoperability and conformance to standards for the life cycle of components; or produce a plan to ensure compliance with standards. As a result, SBA has limited assurance that IDMS meets Federal requirements.

SBA Did Not Fully Satisfy the Requirements of the Second Milestone

FIPS 201-1 and Special Publication 800-79-1 require that Federal agencies obtain a C&A of the security and reliability of their PIV card systems prior to deployment. This review involves a comprehensive assessment to determine the extent to which security controls are implemented correctly, operating as intended, and producing the desired outcome. C&A implementation guidance is

found in NIST SP 800-37, *Guide for the Security C&A of Federal Information Systems*.

Although SBA deployed IDMS in October 2006, it had not completed all of the following three C&A activities prior to deployment:

- A completeness check of the system documentation;
- A certification by an independent third party on the adequacy of system security controls; and
- An accreditation decision, either accepting the level of risk identified by the certification process, denying authority to operate, or imposing restrictions on system operations.

In October 2006, SBA issued a 6-month *Interim Authority to Operate* IDMS, noting that it had not completed the system documentation needed for a complete C&A, specifically, a security risk assessment. This interim authority provided limited authorization to operate IDMS under specific terms and conditions due to outstanding security vulnerabilities.

The initial interim authority also noted that while SBA had prepared a System Security Plan, it did not contain all of the information that must be completed prior to proceeding with the C&A review, according to NIST requirements.¹ Based on interviews with SBA's staff, the Agency had not reviewed security controls and identified security vulnerabilities prior to issuing the *Interim Authority to Operate*. Despite this, SBA allowed personal identity information to be loaded into IDMS and issued PIV cards from the system. In April 2007, SBA issued a second 6-month *Interim Authority to Operate* when the initial one had expired. At that time, the Agency still had not completed any of the three C&A activities.

Moreover, since IDMS was placed into operation, it has undergone multiple software and hardware changes, none of which have been tested to determine the impacts on system security. For example, in February 2008, SBA migrated to new IDMS software and deployed new Public Key Infrastructure (PKI) certification authority without performing acceptance testing to ensure that these applications were secure.

By issuing the interim operating authorities without performing the required C&A review activities, SBA allowed an unstable IDMS to operate with PIV information, which was not adequately protected, as required by Federal guidance. Since SBA did not properly assess the HSPD-12 system, the Agency

¹ NIST SP 800-37.

was also not in a position to know how system vulnerabilities translated into agency-level risk, and whether the level of risk was acceptable before allowing the system to operate.

Further, as of August 29, 2008, SBA was in the process of completing system documentation so that a certification review could be performed. However, because IDMS contains PIV data and has not undergone a full C&A review, continued operation of the system presents an unacceptable level of risk to the Agency and other Federal entities. Consequently, SBA should immediately cease IDMS operations, as required by the June 2008 NIST guidance, and take steps to secure all of the C&A reviews required of NIST 800-79-1 and FIPS 201-1.

SBA Did Not Fully Meet Third Milestone and Will Not Meet the Fourth Milestone

OMB requires that agencies verify and/or complete background investigations and issue PIV cards for contractors and those employees with less than 15 years of service by October 27, 2007. However, as of June 30, 2008, SBA had issued only 379 employee PIV cards and no cards to any of its 312 contractors. Further, SBA officials had not identified the number of employees that had less than 15 years of service. Therefore, we could not determine whether SBA issued PIV cards to all employees that should have been issued identity cards by the October 27, 2007 deadline. However, 379 is such a small fraction of the 4,500 SBA employees that it is unlikely that all employees with less than 15 years of service were issued identity cards.

SBA is also not on schedule to meet the fourth requirement—the issuance of identification cards for all employees with more than 15 years of service—which must be implemented by October 27, 2008. To meet this requirement, SBA will have to issue cards to its remaining 4,121 employees, and also issue cards to the 312 contractors, who did not receive cards by October 27, 2007. Currently, the Agency estimates that this requirement will not be completed until December 31, 2009, or 15 months after the required implementation date.

IDMS Was Not Developed in Accordance with SBA’s System Development Methodology, Resulting in Performance and Reliability Issues

SBA Standard Operating Procedure 90 51 4, *The Office of the Chief Information Officer*, establishes SBA’s System Development Methodology (SDM) as the framework for developing information management systems and maintaining them throughout their life cycle. This methodology is based on OMB Memorandum M-05-23, *Improving Information Technology (IT) Project Planning and Execution*. The purpose of the SDM approach is to ensure that

systems development projects satisfy user requirements, within determined cost, schedule, and quality guidelines.

Despite Agency policy, SBA did not follow the SDM framework when developing and implementing IDMS, including:

- Ensuring that HSPD-12 requirements were incorporated into the IDMS design specifications and adhering to other documentation and activity requirements of the SDM methodology throughout the project's developmental phases; and
- Using Earned Value Management techniques to manage project performance against baseline cost, schedule and performance goals as required by the SDM framework.²

SBA Did Not Follow SDM Project Development Requirements When Developing IDMS

As shown in Table 1, SBA's *System Development Manual* identifies the documents and activities that the SDM framework indicates are critical to each of the six major systems development life cycle phases.

² OMB M-05-23, *Improving Information Technology (IT) Project Planning and Execution*.

Table 1. Development Lifecycle and Document Requirements³

Phase	SDM Documents
Initiate	Needs Statement Business Process Definition and Requirements Feasibility Study Cost/Benefit Analysis Project Plan Risk Assessment System Decision Paper
Define	Functional Requirements Document Logical Database Design (fully attributed) System Security Plan
Design	Technical Specifications Physical Database Design Traceability Matrix Test Strategy Training Plan/Guide IV&V Test Plan
Build	User's Manual Test Analysis Report Installation and Conversion Plan
Evaluation	Test Results and Evaluation Report Project Review
Operate	System Problem Reports

Source: SBA's *Systems Development Methodology*

In developing IDMS, SBA did not maintain or complete many of the documents and activities outlined in the SDM framework, most notably the Project Plan, Functional Requirements Document, Traceability Matrix, and Test Strategy. For example, SBA never completed a Project Plan, which is used to manage all project activities, including the cost, schedule, and technical parameters of the project. SBA also did not finalize the IDMS Functional Requirements Document. This document provides detailed specifications that will support technical interoperability among PIV systems of Federal departments and agencies as well as describes the card elements, system interfaces, and security controls.

Because the Functional Requirements Document had not been prepared, SBA also was not able to complete a Traceability Matrix, which ensures that all requirements in the functional specifications are carried through to the design, build, and evaluation phases. In recognition of the importance of the matrix to the HSPD-12 project's success, GSA developed a FIPS 201 Traceability Matrix

³ Source: SBA IT Project Management Best Practice

specifically for use in the development of PIV card issuance systems. However, SBA did not use the GSA matrix or any other matrix when designing IDMS.

Lastly, SBA did not develop a Test Strategy for IDMS—a crucial step in the SDM framework. This document identifies the minimum operational and performance criteria that each segment of IDMS must meet for it to be accepted as “fit for use” by the Agency. It also includes testing methods and tools that will be used, test cycle performance activities to identify and correct errors, and a final System Acceptance Test to be performed during the Evaluation phase of the project’s development to demonstrate that the system meets the defined requirements. By not developing and implementing a Test Strategy as prescribed by the Agency’s SDM guidance, the Agency has also not complied with NIST guidance on implementing the HSPD-12 requirements. FIPS 201-1 states that “It is the implementer’s responsibility to ensure that components, interfaces, communications, storage media, managerial processes, and services used within the identity verification system are designed and built in a secure manner.”

Because SBA did not follow its own SDM methodology framework, IDMS was deployed with many performance and operational issues that have not been corrected. For example, according to project status reports, IDMS has experienced server freezes, data integrity issues, user processing bottlenecks, problems capturing and verifying fingerprints, among other issues; and lacks a documented data backup and recovery process. For example, a February 2008 software modification rendered the display of employee photos on the IV card unreadable by the new system, and a software patch was installed to correct the issue. Despite these major performance issues, there is no evidence that these problems were corrected. Consequently, the Agency has no assurance of the system’s reliability and ability to fulfill the requirements of the HSPD-12 directive. SBA may also incur substantial rework costs in ensuring IDMS conforms to Federal requirements.

Although IDMS has already been deployed and it is too late in the development cycle to complete all of the SDM requirements for the project initiation, define and design stages, at a minimum SBA should develop and execute a Test Strategy to ensure that the system conforms to all of the Federal performance requirements.

Earned Value Management Techniques Were Not Fully Deployed

In addition to not following SBA’s SDM policy for managing systems development activities, the Agency did not employ basic Earned Value Management controls to manage project cost, schedule and technical

performance, as prescribed by the SDM policy and its *Capital Planning Investment Control* procedures. Earned Value Management is a project management tool that allows visibility into technical, cost, and schedule planning and performance for major Information Technology (IT) projects. It provides assurance that the cost, schedule, and technical aspects of the project are truly integrated and that the actual progress of the project can be identified. Major IT projects are those that cost \$200,000, more in a single year or \$500,000 or more in 3 years, or are deemed to be of high visibility. SBA's SDM policy mandates that all major IT projects use an Earned Value Management system.

SBA's policy is based on OMB guidance, which requires the use of Earned Value Management techniques for all major IT investments with development work, and requirements of the Federal Acquisition Streamlining Act of 1994⁴ and the Clinger-Cohen Act of 1996.⁵ The Federal Acquisition Streamlining Act requires agency heads to achieve, on average, 90 percent of the cost and schedule goals established for major and non-major acquisition programs and the Clinger-Cohen Act requires the establishment of processes for agencies to analyze, track, and evaluate the risks and results of major investments in IT.

Despite these requirements, SBA did not use Earned Value Management techniques or establish an effective and efficient capital planning processes for selecting, managing, and evaluating the results of its investment in IDMS. Also given the performance issues noted previously, it is unclear how much additional investment will be required in IDMS to meet the secure and reliable performance requirements of HSPD-12.

SBA staff explained that it did not consider IDMS to be a major system or a technology project. For this reason they did not follow the SDM framework or use an Earned Value Management approach in managing the project.

SBA Did Not Report the IDMS Project to OMB through the Exhibit 300 Process

OMB Circular A-11 establishes policy for planning, budgeting, acquisition and management of Federal capital assets, and instructs agencies on budget justification and reporting requirements for both major IT investments and non IT capital assets. The circular requires major IT investments to be approved as capital projects through the OMB Exhibit 300 process. As defined previously, major IT investments are those costing \$200,000, more in a single year or \$500,000 or more in 3 years. Under the Exhibit 300 process, the Agency reports to OMB the project's scope, schedule and cost objectives, a baseline plan for

⁴ Public Law 103-355

⁵ Public Law 104-106

accomplishment of program objectives, and an Earned Value Management assessment of actual performance against the objectives.

Although the current \$3.3 million price tag of IDMS clearly qualified it as a major IT investment, SBA did not comply with OMB budgeting requirements to report IDMS as a capital project through the Exhibit 300 process. Instead, the project was financed entirely out of operating funds, and the \$3.3 million IT investment was not separately identified in the Agency's budget. As explained above, SBA staff managing the project did not consider IDMS to be a major IT project subject to the Exhibit 300 reporting requirement.

Because it is unclear how much additional investment in IDMS will be required to correct performance and security problems, and because the project constitutes a major IT investment, SBA should use Earned Value Management techniques to manage project performance and report to OMB, through the Exhibit 300 process, a baseline plan for accomplishment of the project's objectives.

RECOMMENDATIONS

We recommend the Associate Administrator for Management and Administration work with the Chief Information Officer to:

1. Immediately cease IDMS operations, as required by the June 2008 NIST guidance, until the Agency complies with HSPD-12 C&A requirements and can ensure that IDMS system is capable of protecting the privacy data it contains.
2. Implement the provisions of NIST 800-79-1 and FIPS 201-1 by securing a C&A of the Agency as a PIV Card Issuing Organization; an accreditation of all HSPD-12 products and services provided by third parties; and a security C&A of IDMS.
3. Develop and execute a Test Strategy to ensure that IDMS meets all of the HSPD-12 functional requirements, including reading and authenticating the digital certificates on identity cards.
4. Deploy Earned Value Management techniques to establish project cost, schedule and performance goals and to manage the project within 90 percent of the baselines.
5. Complete an Exhibit 300, *Capital Asset Plan and Business Case*, for IDMS to establish a baseline plan for accomplishment of the project's objectives and submit it to OMB, as required.

AGENCY COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

On September 11, 2008, we provided a draft of this report to SBA for comment, and received written comments from Chief Information Officer and Associate Administrator for Management and Administration on October 2, 2008. The response partially disagreed with recommendation 1, agreed with recommendations 2 and 5, and disagreed with recommendations, 3 and 4. These comments, along with our response, are summarized below. The full text of management's comments can be found in Appendix II.

General Comments

Management commented that the OIG report does not accurately reflect the Agency's efforts to implement HSPD-12, asserting that:

- The report statement that \$3.3 million had been spent on HSPD-12 does not reflect that the expenditures included the acquisition of hardware and software, software integration, and project management consultant services.
- The HSPD-12 software upgrade affected only the display of the employee photo on the PIV card and did not make all PIV cards unreadable.
- Although a number of documents were provided to the OIG as evidence of SBA's compliance with OMB guidance regarding security C&A and Earned Value Management, it appears that the documentation did not receive a thorough review prior to the draft being issued.

OIG Response

To address the first two assertions, we added a description of what the \$3.3 million in expenditures included, and revised the report language to clarify that the display of employee photos was impacted by the software upgrade. We disagree with management's third assertion, and believe the report accurately reflects the Agency's progress in implementing the HSPD-12 initiative. The documentation that SBA provided during the audit did not demonstrate that the Agency had undergone a C&A review of its organization; performed a security C&A of IDMS to demonstrate that the system is secure and reliable, or followed its own requirements to use earned value management in planning and managing the IDMS project. Moreover, the OIG made repeated attempts to obtain support for the Agency's assertions, but the OCIO was unable to produce

evidence of its compliance, and in its response to this report, acknowledged that it had not completed a C&A of IDMS.

Further, during discussions with SBA on the audit findings, the OCIO identified a number of alternative actions taken, which it believed could be substituted for the specific actions called for in the initiative. We disagree that the alternative actions can be interpreted as satisfying the HSPD-12 requirements, and believe the guidance is very specific on what actions needed to be completed to implement the initiative. For example, management stated that IDMS was PIV-I compliant because it was a pilot system and did not require a full security C&A. Also, as a result of an early-on engagement with GSA, the Agency's system was fully vetted and deemed compliant with NIST guidance.

However, FIPS 201-1 and Special Publication 800-79-1 require that Federal agencies obtain a C&A of the security and reliability of their PIV card systems prior to deployment. This review involves a comprehensive assessment to determine the extent to which security controls are implemented correctly, operating as intended, and producing the desired outcome. Also, the guidance does not suggest that the card system can be treated as a pilot project or that the C&A requirements can be waived. To-date, SBA has still not completed a C&A of IDMS. Moreover, since IDMS was placed into operation, it has undergone multiple software and hardware changes, none of which have been tested to determine the impacts on system security.

Recommendation 1

Management's Comments

Management partially disagreed to cease production of PIV card, stating that an early-on engagement with GSA deemed the Agency's system to be compliant with the NIST requirements, and that a full C&A was not required because the system was deployed as a pilot. Further, the Agency is pursuing a security C&A of the system and has fully addressed several vulnerabilities that were identified as a result of a risk assessment.

OIG Response

On June 30, 2008, NIST issued an update of SP 800-79, emphasizing the importance of determining whether card issuing organizations are capable of performing the card issuance services required of HSPD-12. This guidance further states that card issuing organizations should issue PIV cards only after they have been authorized to operate based on the assessment criteria outlined in SP 800-79-1. More importantly, the publication stresses that agencies that have started issuing PIV cards, but which do not meet the accreditation guidance, should immediately halt card issuance operations.

Based on this very specific and clear guidance, we do not believe that SBA is justified in its decision to continue issuing PIV cards, especially given the highly sensitive personal information processed by the IDMS application. Consequently, we will seek a management decision on this recommendation through the audit resolution process.

Recommendation 2*Management's Comments*

Management agreed to secure a C&A of IDMS based on NIST 800-79-1 and FIPS 201-1.

OIG Response

Although management concurred with the recommendation, its comments were not fully responsive. While agreeing to complete the Security C&A for IDMS required by NIST 800-37, SBA's response does not address or provide a timeline as to when it will meet the additional criteria outlined in SP 800-79-1, such as securing a C&A of its card issuing organization, and obtaining accreditation for products and services provided by third parties. Consequently, we are requesting that SBA provide additional comments addressing the full recommendation.

Recommendation 3*Management's Comments*

Management disagreed with recommendation 3, stating that it executed a comprehensive Test Plan in conjunction with the systems integrator.

OIG Response

We disagree with management's response as SBA was unable to provide the OIG with the Test Plan it claims it has executed, or with any other acceptance test plans for IDMS. Consequently, we will pursue a management decision on the recommendation the audit resolution process.

Recommendation 4*Management's Comments*

Management disagreed with the recommendation, stating that the HSPD-12 project was subject to the full range of Earned Value Management to ensure effective management and administration of the project.

OIG Response

We disagree with management's assertion. None of the project planning and execution documents or contractor reports reviewed during the audit contained Earned Value Management analysis or measurements. Moreover, project officials interviewed told us that they did not perform an Earned Value Management analysis or use such measures to manage the project. Consequently, we will seek a management decision on this recommendation through the audit resolution process.

Recommendation 5*Management's Comments*

Management agreed with the recommendation and state that it has contracted with a company to complete an Exhibit 300 for HSPD-12 in the second quarter of FY 2009.

OIG Response

We found management's comments to be responsive to the recommendation.

ACTIONS REQUIRED

Because your comments did not fully address recommendation 2, we request that you provide a written response by October 20, 2008, providing additional details and target dates for implementing the recommendation.

We appreciate the courtesies and cooperation of the Office of the Chief Information Officer and the Office of Management and Administration during this audit. If you have any questions concerning this report, please call me at (202) 205-[FOIA Ex. 2] or Jeffrey Brindle, Director, Information Technology and Financial Management at (202) 205-[FOIA Ex. 2].


APPENDIX I: AUDITEE COMMENTS



U.S. SMALL BUSINESS ADMINISTRATION
WASHINGTON, D.C. 20416

Date: October 2, 2008

To: Debra S. Ritt
Assistant Inspector General for Auditing

From:  Robert F. Danbeck [FOIA Ex. 6]
Associate Administrator for Management and Administration

Christine H. Liu [FOIA Ex. 6]
Chief Information Officer

Subject: Response to the Office of The Inspector General - Draft Report on SBA's Implementation of an HSPD-12 Card Issuance System (Project No. 8001)

This memo responds to the Office of The Inspector General's "Draft Report on SBA's Implementation of Homeland Security Presidential Directive-12 (HSPD-12) Card Issuance Systems (Project No. 8001)" dated, September 11, 2008.

The Office of the Chief Information Officer (OCIO) and the Office of Management and Administration (M&A) have closely collaborated to ensure effective oversight and implementation of the Presidential HSPD-12 initiative. The OIG audit report does not accurately reflect SBA's efforts to implement this program. While the report highlights several recommendations that we jointly agree on the actions required to effectively implement the HSPD-12 program, our review identified a number of inaccurate statements throughout the report.

The report states that SBA spent a total of \$3.3 million that resulted in the deployment of 379 identity cards. This statement does not accurately reflect that the stated expenditures include (1) the acquisition of the hardware and software infrastructure, (2) software integration, and (3) project management consulting services to implement the program.

In February 2008, SBA implemented a HSPD-12 software upgrade that affected the display of the employee photo on the PIV card, and a software patch was quickly implemented to correct this issue. The report inaccurately states that "in February 2008, the HSPD-12 software was modified and resulted in rendering all previously issued PIV cards unreadable by the system".

Although a number of documents were provided to the OIG as evidence of SBA's compliance with OMB guidance regarding security certification and accreditation (C&A) and earned value management (EVM), it appears that the documentation did not receive a thorough review prior to the draft being issued.



While SBA has made considerable progress towards implementing this unfunded program in a very tight budget constrained environment, the report, as written, does not address the fact that SBA was one of 6 Federal agencies that successfully passed the Department of Homeland Security HSPD-12 interoperability exercises (e.g., Winter Blast and Summer Breeze). These PIV credential interoperability exercises clearly confirmed SBA's credential meets the FIP 201-1 interoperability requirement, and that SBA's card interoperated with other agencies. As a result of SBA's PIV credential successful interoperability test results, FEMA partnered with SBA in the legislatively mandated initiative to implement the Emergency Support Functions for Federal Emergency Response Officials (FERO) First Responders repository.

While the subject draft audit report findings were many and focused on several broad general areas concerning security, privacy, systems development methodology, funding, earned value management, NIST standards, and OMB requirements, for purposes of clarity, we have specifically focused on the following 5 OIG recommendations made to the Chief Information Officer. We propose recommendations 4 and 5 be combined and that the report be issued jointly to the CIO and the Associate Administrator for Management and Administration:

Recommendations #1: Immediately cease IDMS operations, as required by the June 2008 NIST guidance, until the Agency complies with HSPD-12 certification and accreditation requirements and can ensure that IDMS system is capable of protecting the privacy data it contains.

Response: We partially disagree with OIG's recommendation number 1. As a result of an early-on engagement with GSA, the agency's HSPD-12 implementation was fully vetted and deemed compliant with NIST FIPS 201-1. Subsequently, SBA PIV card and its configuration were validated by GSA in May 2007.

With respect to the HSPD-12 Certification and Accreditation (C&A) system level requirements contained in Special Publication (SP) 800-79-1, SBA was unable to comply with this requirement since the SP was just published in June 2008. SBA issued an Interim Authority to Operate (IATO) for HSPD-12 because at the time this new requirement did not exist. Moreover, the system was deployed as a pilot, and as such, a full C&A was not required. Subsequently, SBA conducted a risk assessment and several vulnerabilities were identified, which were fully addressed to mitigate the risks.

The system-level controls (as part of the C&A process) have been completed. We are on schedule to complete a review of the physical data center security controls in FY09, QTR1. A Privacy Impact Assessment (PIA) has been completed to assess the data contained in the IDMS.

The aggregated components consisting of the (1) system-level controls, (2) physical data center security controls, and (3) PIA, will complete the C&A package for IDMS, targeted for early FY09, QTR1.

Recommendation #2: Implement the provisions of NIST 800-79-1 and FIPS 201-1 by securing a certification and accreditation of the Agency as a PIV Card Issuing Organization; an accreditation of all HSPD-12 products and services provided by third parties; and a security certification and accreditation of IDMS.

Response: We agree with recommendation number 2 in securing a C&A of IDMS based on NIST 800-79-1 and FIPS 201-1. SBA has already initiated the required actions to complete a certification and accreditation of the IDMS by FY09, QTR1. SBA will also initiate securing a C&A of the Agency as a PIV card issuing organization.

Recommendation #3: Develop and execute a Test Strategy to ensure that IDMS meets all of the HSPD-12 functional requirements, including reading and authenticating the digital certificates on identity cards.

Response: We disagree with recommendation number 3. In conjunction with the IBEX, Inc, the HSPD-12 systems integrator, approved products were purchased from the June 30, 2006 list of OMB approved products. SBA, in conjunction with the Integrator developed and executed a comprehensive Test Plan to ensure proper integration of the functional requirements, including reading and authenticating the digital certificate on the PIV credential. In May 2007, GSA validated that SBA PIV credential fully complied with NIST 800 series standards and met the interoperability requirements across the Federal bridge.

In addition, SBA was one of a 6 Federal agencies that successfully passed the Department of Homeland Security HSPD-12 PIV credential interoperability exercises (e.g., Winter Blast and Summer Breeze).

Recommendation #4: Deploy Earned Value Management techniques to establish project cost, schedule and performance goals and to manage the project within 90 percent of the baselines.

Response: We disagree with recommendation number 4. During the HSPD-12 project life-cycle, it has been presented to the SBA IT Governance review and approval process 12 times. In each case, the project was subject to the full range of earned value management EVM to ensure effective management and administration of the project.

In addition, in order to accurately assess the full cost as well as the schedule of the HSPD-12 program, we recommend that OHCM and OIG jointly undertake an initiative to implement an automated information system solution that accurately captures SBA employees' years of Federal service to satisfy HSPD-12 implementation requirements set forth in OMB M-08-01. This automated system is necessary for ensuring SBA's effectiveness in complying with OMB's HSPD-12 implementation requirements.

Recommendation #5: Complete an Exhibit 300, Capital Asset Plan and Business Case, for IDMS to establish a baseline plan for accomplishment of the project's objectives and submit it to OMB, as required.

Response: We agree with recommendation number 5. M&A has contracted with the LS3 Corporation to complete an Exhibit 300 for HSPD-12 in FY09, QTR 2.

We appreciate the opportunity to provide comments on the proposed HSPD-12 draft audit. If you have any questions, please contact Kenneth Etheridge at (202) 205-[FOIA EX 2] or Ravoyne Payton at (202) 205 [FOIA EX 2]