NATIONAL CREDIT UNION ADMINISTRATION
OFFICE OF INSPECTOR GENERAL

REVIEW OF THE IMPLEMENTATION OF HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 12

Report #OIG-08-06 June 4, 2008

William A. DeSarno
Inspector General

Released by:

James Hagen
Deputy IG for Audits

Auditor-in-Charge:

W. Marvin Stith, CISA
Senior Information Technology Auditor

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The National Credit Union Administration (NCUA) Office of Inspector General (OIG) performed an audit to determine the status of NCUA's implementation of Homeland Security Presidential Directive – 12 (HSPD-12) - Policy for a Common Identification Standard for Federal Employees and Contractors. To determine NCUA's status in implementing HSPD-12, we interviewed management and staff from the NCUA Office of the Chief Information Officer (OCIO), Office of Human Resources (OHR), Office of General Counsel (OGC), and the Office of the Chief Financial Officer (OCFO) Division of Procurement and Facilities Management (DPFM). We also interviewed a representative from the General Services Administration (GSA). In addition, we reviewed HSPD-12 policies and requirements, as well as NCUA documentation, procedures and policies regarding HSPD-12 implementation.

We determined NCUA has made progress towards issuing Personal Identity Verification (PIV) credentials to its employees and contractor employees. NCUA has verified, initiated, or completed background investigations on its employees. In addition, NCUA has begun initiating background investigations on its contractor employees. Furthermore, NCUA proofed and registered[1] its existing employees and contractor employees starting in August 2006. However, NCUA has not issued credentials to new or existing employees and contractor employees as required, and the credentials NCUA plans to issue do not meet HSDP-12 and Federal Information Processing Standard 201 (FIPS 201) requirements. In addition, NCUA has not fulfilled other HSPD-12 requirements. Specifically, NCUA:

- Does not have an implementation plan;
- Does not have an accredited and approved identity proofing and registration process;
- Does not have an accredited and approved PIV issuance and management process; and
- Has not included language in contracts requiring compliance with HSPD-12 and FIPS 201

We made eight recommendations where improvements could be made. Management agreed with seven of the recommendations and is taking corrective action or has plans to address the recommendations. Management disagreed with the recommendation to place a federal cross-certified certificate on the credentials and made a business decision to only place the certificate on senior NCUA staff credentials. Management believes that given limited interoperability with other federal agencies and the significant cost per certificate involved, the expenditure of NCUA funds for the cross-certified certificate is not justified for all employees at this time. A complete copy of management's formal written response is attached as an appendix to this report.

[1] Identity proofing and registration are the activities involved in verifying identities and recording that information.

BACKGROUND:

On August 27, 2004, the President signed HSPD-12, which provides policy guidelines to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and contractors (including contractor employees). "Secure and reliable forms of identification" for purposes of this directive means identification that (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process.

On February 25, 2005, the Secretary of Commerce approved and issued Federal Information Processing Standard 201, Personal Identity Verification of Federal Employees and Contractors (FIPS 201). The National Institute of Standards and Technology (NIST) developed this standard to satisfy the requirements of HSPD-12. The Office of Management and Budget (OMB) is responsible for ensuring compliance with HSPD-12. On August 5, 2005, OMB issued a memorandum (M-05-24) that provided instructions to agencies for implementing HSPD-12 and FIPS 201. According to M-05-24, HSPD-12 requires agencies to conduct a background investigation, adjudicate the results, and issue identity credentials to their employees and contractors who require long-term access to federally controlled facilities or information systems. However, it does not apply to individuals under contract to a department or agency, who require only intermittent access to federally controlled facilities.

FIPS 201 is composed of two parts: PIV-I and PIV-II. PIV-I describes the minimum requirements for a federal personal identification system that meets the control and security objectives of HSPD-12, including personal identity proofing, registration, and issuance. PIV-II provides detailed technical specifications to support the control and security objectives in PIV-I as well as interoperability among federal departments and agencies. PIV-II describes the policies and minimum requirements of a PIV Card that allows interoperability of credentials for physical access and logical access.

OBJECTIVE:

The objective of this review was to assess the status of NCUA's implementation of HSPD-12.

SCOPE & METHODOLOGY:

To determine the status of NCUA's implementation of HSPD-12, we interviewed management or staff from the NCUA OCIO, OHR, OGC, and OCFO DPFM. We also interviewed a representative from the GSA. In addition, we reviewed HSPD-12 policies and requirements, and NCUA documentation, procedures and policies regarding HSPD-12 implementation.

We conducted our fieldwork from February 2008 through May 2008 and performed this review in accordance with Generally Accepted Government Auditing Standards.

RESULTS:

A. NCUA did not meet OMB milestones for issuing credentials

NCUA has made progress towards issuing PIV credentials to its employees and contractor employees. OHR verified, initiated, or completed employee background checks and has begun pursuing contractor background investigations. OHR also proofed and registered existing NCUA employees and contractor employees starting in August 2006. However, NCUA has not issued credentials to new or existing employees and contractor employees as required. OMB required agencies to:

- Begin issuing credentials to *new* employees and contractor employees by October 27, 2006; and

- Issue and use credentials for *current* employees and contractor employees by October 27, 2007

In addition, FIPS 201 required that the identity credentials agencies issue to individuals without a completed background investigation must be electronically distinguishable from identity credentials issued to individuals who have a completed investigation.

NCUA reported to OMB that as of September 2007, it had 942 employees that required PIV credentials. NCUA also reported that all its employees had completed or adjudicated background investigations.[2] However, NCUA had issued only one credential. NCUA reported to OMB that it had issued only 10 credentials as of December 2007. In addition, as of May 6, 2008, OHR indicated it had 40 contractor employees on staff requiring background investigations and had initiated the paperwork for 23 of these contractor employees.[3] NCUA indicated that technology issues impacted its ability to produce PIV credentials.

While NCUA did not meet required OMB milestones for issuing its credentials, OMB indicated, on October 26, 2007, that no federal agency would meet the October 27, 2007 deadline. OMB reported that as of March 1, 2008, federal agencies had issued credentials to approximately three percent of employees and three percent of contractor employees. OMB indicated that unexpected technical difficulties caused agencies to miss the goal.

[2] NCUA indicated to the OIG in April 2008 that it had one employee who entered on duty in March 2004 who did not have an initial background investigation. In addition, NCUA identified six employees who entered on duty between April and September 2007 for whom NCUA submitted their investigation paperwork to OPM prior to their entry on duty.

[3] For the purposes of this audit, we are defining "initiated" as the employee at least completed the paperwork and provided it to OHR.

Considering the status of the majority of the federal community in issuing credentials, we did not consider that NCUA's status would have any adverse impact regarding the HSPD-12 goal for interoperability among federal departments and agencies. Therefore, we are not making a recommendation regarding this issue at this time

B. The PIV credentials NCUA plans to issue do not meet HSPD-12 requirements

NCUA has made progress towards issuing credentials, and NCUA indicated to OMB in January 2008 that it would create credentials for all employees by March 31, 2008. However, the NCUA credential as configured does not incorporate the certificate required by FIPS 201. In addition, GSA had not validated the NCUA credential as configured.

OMB allows agencies to place additional certificates on its credentials. However, it mandates that a digital certificate be incorporated on the credential for access control that originates from:

- An agency certification authority[4] cross-certified with the Federal Bridge Certificate Authority (FBCA[5]) at medium assurance or higher; or

- An approved Shared Service Provider.

OCIO configured the NCUA credential with a Microsoft[6] certificate that will allow NCUA users to access the NCUA VPN, but which is not cross-certified with the FBCA. OCIO indicated it did not put the federal certificate on its credentials because: (a) of the cost of procuring and maintaining a cross-certified certificate, and (b) the functionality for using the federal certificate is not yet available and therefore is not an issue. OCIO indicated it could add the certificate when the functionality for the certificate is available. However, OCIO recently decided to configure credentials for all NCUA Board members and executive staff with the federal certificate before the agency issues the credentials.

In addition, GSA did not validate the credential NCUA planned to issue with the Microsoft certificate. OMB required agencies to provide credentials with their agency's standard configuration to GSA for testing. GSA validated an NCUA credential in September 2007. However, the credential contained a certificate other than the Microsoft certificate NCUA plans to use. The GSA representative responsible for the testing indicated that when an agency changes certificates after GSA validated the credential, the agency should submit the updated credential for

[4] A certification authority is a trusted third party that issues digital certificates and validates the identity of the holder of a digital certificate.
[5] The FBCA allows an entity to accept digital identity certificates issued by other entities for transactions. It allows for trust between different agencies regardless of which entities are involved in the sharing of information.
[6] Microsoft is not an approved Shared Service Provider.

revalidation. We discussed this issue with OCIO, and OCIO indicated it would provide another credential to GSA.

Issuing a credential that meets federal requirements will ensure NCUA's ability to fulfill the HSPD-12 goals for a secure and reliable form of identification that is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation and that can be rapidly authenticated electronically. In addition, it would ensure NCUA credentials meet the HSPD-12 goal for interoperability of credentials for physical and logical access control. Furthermore, we believe that creating and issuing credentials before NCUA incorporates the federal certificate could lead to logistical challenges for NCUA because the majority of NCUA employees are located in four Regional offices and the Asset Management Assistance Center (AMAC), which are geographically dispersed from the Central Office where NCUA issues and maintains the credentials. [7]

Recommendation #1: Prior to issuing its credentials, NCUA should incorporate a federal certificate on its credentials that is cross-certified with the Federal Bridge Certificate Authority.

Management Response: Management disagreed with our recommendation. Management believes that given limited interoperability with other federal agencies and the significant cost per certificate involved, the expenditure of NCUA funds for the cross-certified certificate is not justified for all employees at this time. However, management also indicated it would load a limited number of cross-certified certificates on the PIV credentials of senior NCUA staff.

OIG Response: We understand that NCUA is making a business decision to not configure all its credentials with the cross-certified federal certificate at this time based on the cost-benefit. We do not plan to pursue this matter in resolution.

Recommendation #2: Prior to issuing its credentials, NCUA should submit a credential with the required certificate configuration to GSA for testing.

Management Response: Management agreed with our recommendation and indicated it is in the process of submitting the updated credential configuration to GSA prior to issuing the PIV cards.

OIG Response: We agree with the proposed action.

Recommendation #3: NCUA should issue its credentials as soon as practicable after fulfilling the two recommendations above.

[7] The four Regional offices are located in New York, Georgia, Arizona, and Texas, and AMAC is also located in Texas.

Management Response: Management agreed with our recommendation. Management indicated it would issue credentials to all central and regional office staff after GSA tests the credential configuration. Specifically, management indicated it would issue credentials to field staff at the upcoming NCUA regional conference in September.

OIG Response: We agree with the proposed action.

C. NCUA does not have an HSPD-12 Implementation Plan

At OMB's request, NCUA provided its initial implementation status to OMB in June 2005 and an updated status in September 2006. However, NCUA does not have an implementation plan. In May 2005 when OMB requested agencies provide their implementation status by June 27, 2005, it informed agencies they needed to prepare a detailed implementation plan. In addition, when OMB published its overall HSPD-12 implementation guidance in August 2005, it listed the implementation plan as a requirement that agencies were supposed to provide to OMB by June 27, 2005. NCUA does not have an implementation plan because there is no single NCUA office responsible for directing and coordinating the various functional components involved in implementing the HSPD-12 program for the agency.

Several NCUA offices have responsibilities for implementing HSPD-12 such as OCIO, OHR, and OCFO. However, no single office has accepted the overall responsibility for directing and coordinating the implementation of HSPD-12 for the agency as a whole.

While OCIO and OCFO DPFM have considered and made efforts towards physical and logical access solutions, the agency may have been able to pursue or implement more timely access solutions if it had prepared an implementation plan. For example, OCIO could have established a budget and timeline to procure a certificate that is cross-certified with the FBCA for logical access control to federally controlled information systems. In addition, OCFO DPFM could have detailed a solution, timeline and budget for physical access to NCUA facilities in an implementation plan.

Regarding NCUA's physical access solution, OCFO DPFM began pursuing a card reader in 2007 for building access under HSPD-12 to replace NCUA's existing HID[8] devices that would be able to read both its legacy building access cards and the new PIV credentials. Recently, OCIO learned that PIV cards which function with NCUA's existing HID card readers were on the GSA approved products list.[9] These cards could potentially provide NCUA with a physical access solution under HSPD-12 without having to replace the existing readers. OCIO had planned to obtain and test

[8] HID is a manufacturer of secure identity solutions and contactless smart card technology for physical access control.
[9] These cards have been on the GSA Approved Products List since September 2006.

some of these PIV cards as a potential solution. However, OCIO indicated they assessed the cards as a potential solution and determined they were too costly.

In addition, an implementation plan could have outlined NCUA's timeline to fulfill other HSPD-12 requirements it has not met, such as:

- Accrediting and approving an identity proofing and registration process (See Finding D below);

- Accrediting and approving a PIV issuance and management process (See Finding D below); and

- Incorporating language into contracts requiring contractor compliance with HSPD-12 and FIPS 201(See Finding E below)

Recommendation #4: NCUA's Executive Director should designate a single office with overall responsibility for directing and coordinating HSPD-12 implementation for NCUA.

Management Response: Management agreed with our recommendation and designated the NCUA Office of Human Resources (OHR) as the office responsible for HSPD-12 implementation.

OIG Response: We agree with the proposed action.

Recommendation #5: NCUA should develop a detailed HSPD-12 implementation plan.

Management Response: Management agreed with our recommendation and indicated it has been in the process of developing an implementation plan.

OIG Response: We agree with the proposed action.

D. NCUA does not have accredited and approved procedures for verifying the identities of its employees and contractor employees or for issuing and managing PIV credentials

OHR established and implemented an identity proofing and registration process for employees and contractor employees that meets key FIPS 201 requirements.[10] In October 2005, OHR published training and guidance on the roles, requirements and procedures for proofing and registration and made the training and requirements available on its intranet. In addition, OHR proofed and registered its existing

[10] NCUA's identity proofing and registration process provides for separation of duties, and the process requires applicants to provide two acceptable forms of identity source documents.

employees and contractor employees starting in August 2006. In addition, OHR prepared a "PIV Issuance and Maintenance" process for issuing and managing PIV credentials. However, NCUA has not approved or accredited these processes.

OMB required agencies to adopt and accredit[11] an approved[12] identity proofing and registration process by October 27, 2005. In addition, FIPS 201 requires agencies to accredit and approve their PIV issuance and management procedures. Furthermore, OMB indicated agencies cannot issue new identity credentials until they have approved and accredited procedures.

By accrediting and approving its proofing and registration and its PIV issuance and management procedures, NCUA would facilitate its ongoing ability to meet the HSPD-12 control objective to ensure agencies issue credentials based on sound criteria for verifying an individual employee's identity.

Recommendation #6: NCUA should accredit and approve its identity proofing and registration procedures prior to issuing credentials.

Management Response: Management agreed with our recommendation and indicated OHR is in the process of submitting the written procedures for accreditation and approval prior to issuing the credentials.

OIG Response: We agree with the proposed action.

Recommendation #7: NCUA should accredit and approve its PIV credential issuance and management procedures prior to issuing credentials.

Management Response: Management agreed with our recommendation and indicated it would comply with NIST requirements when it issues its credentials.

OIG Response: We agree with the proposed action.

E. NCUA contracts do not require contractor employee compliance with HSPD-12

NCUA employs contractor employees at its Central Office and its Asset Management and Assistance Center (AMAC). OHR began proofing and registering contractor employees starting in August 2006 and has also begun pursuing background checks on contractor employees. However, NCUA contracts do not include language requiring compliance with HSDP-12 and FIPS-201. OCFO DPFM and AMAC staff responsible for this requirement indicated they were not aware of the requirement.

[11] Agencies must accredit that these processes satisfy FIPS 201 requirements.
[12] The head of the agency must approve the procedures in writing.

OMB required that by October 27, 2005, all new contracts (including exercised options) that require contractors to have long term access to federally controlled facilities or access to federally controlled information systems shall include language requiring compliance with PIV procedures. The Federal Acquisition Regulation includes a clause NCUA could use in its contracts that requires contractors to comply with HSPD-12 and FIPS 201.

By ensuring contractors are required to comply with PIV procedures, NCUA can ensure its contractor employees meet HSPD-12 requirements and continue to provide optimum services to NCUA employees and oversight of the nation's credit unions.

Recommendation #8: NCUA should update its contracts to include language requiring contractor employees to comply with HSPD-12 and FIPS 201.

Management Response: Management agreed with our recommendation and indicated it has taken action to update purchase orders and notify contractors of the requirement to comply.

OIG Response: We agree with the proposed action.

NCUA MANAGEMENT COMMENTS

National Credit Union Administration
Office of Executive Director

Via E-Mail

TO: William A. DeSarno, Inspector General

FROM: Executive Director J. Leonard Skiles

SUBJECT: Response to Draft Report
Review of the Implementation of HSPD-12

DATE: May 29, 2008

Thank you for the opportunity to comment on the Inspector General's draft report entitled *Review of the Implementation of Homeland Security Presidential Directive 12*. Below is a response to each of the eight recommendations in the report.

Recommendation #1: *Prior to issuing its credentials, NCUA should incorporate a federal certificate on its credentials that is cross-certified with the Federal Bridge Certificate Authority.*

Response – As discussed in the report, it is not a sound business decision for NCUA to purchase cross-certified certificates for all employees at this time. We will be loading a limited number of cross-certified certificates on the PIV cards of senior agency staff. As the report notes, due to technical difficulties the vast majority of the federal government and associated systems are not yet capable of accepting the cross-certified certificates. Further, most NCUA staff rarely interact with other government agencies. Thus, given limited interoperability and the significant cost per certificate involved, we do not believe the expenditure of agency funds for the cross-certified certificate is justified at this time. When acceptance of the cross-certified certificate becomes operational, we will update all employees' PIV cards with the cross-certified certificate. Our capability to process new employees within the regional and central office, and our biennial regional conferences for field staff will enable us to address PIV card updates for all employees when the time comes to add the cross-certified certificate.

Recommendation #2: *Prior to issuing its credentials, NCUA should submit a credential with the required certificate configuration to GSA for testing.*

Response – We agree, and are in the process of submitting the updated credential configuration to GSA prior to issuance of the PIV cards. We did submit the initial credential configuration to GSA.

1775 Duke Street – Alexandria, VA 22314-3428 - 703-518-6300

Recommendation #3: *NCUA should issue its credentials as soon as practical after fulfilling the two recommendations above.*

Response – We agree. Our plan is to issue the PIV cards to all central and regional office staff upon completion of testing of the configuration by GSA. We will issue PIV cards to field staff during the upcoming regional conferences in September.

Recommendation #4: *NCUA's Executive Director should designate a single office with overall responsibility for directing and coordinating HSPD-12 implementation for NCUA.*

Response – The Office of Human Resources (OHR) is the designated office for HSPD-12 implementation. OHR is coordinating with and receiving support from our Office of Chief Information Officer and our Office of Chief Financial Officer regarding information technology and facility management issues.

Recommendation #5: *NCUA should develop a detailed HSPD-12 implementation plan.*

Response – We agree and have been in the process of developing an implementation plan now that we have the research and development and technological issues resolved.

Recommendation #6: *NCUA should accredit and approve its identity proofing and registration procedures prior to issuing credentials.*

Response – In accordance with NIST FIPS 201-1, § 2.2, NCUA's identify proofing and registration procedures comply with the requirements for accreditation. In it's identify proofing and registration NCUA:

- Adopted and used an approved identity proofing and registration process for all employees, new hires, and contract employees.
- Required all applicants to provide two forms of original identification, with at least one being a valid State or Federal government-issued picture ID for identify proofing and registration.
- Has or is in the process of having the Office of Personnel Management conduct a NAC, NACI, or other appropriate investigation of all employees, new hires, and contract employees.
- Ensures separation of duties relative to the above procedures, in that staff doing the initial identifying proofing and registration will be different from those issuing the cards. The staff responsible for the background investigations is also different from those issuing PIV cards.

OHR is in the process of submitting the written identity proofing and registration procedures for accreditation by the agency head or its designee. Approval of the procedures will occur prior to issuance of the credentials.

Recommendation #7: *NCUA should accredit and approve its PIV credential issuance and management procedures prior to issuing credentials.*

Response – NCUA has not issued PIV credentials to its employees but when it does it will comply with the requirements in NIST FIPS 201-1, § 2.2 and Attachment A.

Recommendation #8: *NCUA should update its contracts to include language requiring contractor employees to comply with HSPD-12 and FIPS 201.*

Response – We agree. NCUA has taken steps to update the Purchase Order Terms and Conditions page that accompanies all purchase orders so that it includes the Federal Acquisition Regulation citation 52.204-9, Personal Identity Verification of Contractor Personnel. With respect to existing contracts, some contractors have been notified and are in the process of meeting the new requirement. NCUA will notify all appropriate contractors by letter that compliance will be required at contract renewal or with the exercise of an option.

Thank you for the opportunity to comment. If you have any questions, please contact me.

bcc: DED Fazio

S:\DED\2008\OIGDraftHSPD-12.doc