NATIONAL CREDIT UNION ADMINISTRATION
OFFICE OF INSPECTOR GENERAL

REVIEW OF NCUA'S COMPLIANCE WITH OMB M-06-16 PROTECTION OF SENSITIVE AGENCY INFORMATION

Report #OIG-07-01 February 7, 2007

William A. DeSarno
Inspector General

Released by:

James Hagen
Asst IG for Audits

Auditor-in-Charge:

Tammy F. Rapp, CPA, CISA
Sr Information Technology Auditor

TABLE OF CONTENTS

Section		Page
	EXECUTIVE SUMMARY	1
	INTRODUCTION	2
	BACKGROUND	2
	OBJECTIVE	3
	SCOPE & METHODOLOGY	3
	RESULTS	4
A	Confirm identification of personally identifiable information protection needs	4
B	Verify adequacy of organizational policy	8
C	Implement protections for PII transported/stored offsite	8
D	Implement protections for remote access to PII	9
E	Encrypt all data on mobile computers/devices	10
F	Allow remote access only with two-factor authentication	13
G	Use a time-out after 30 minutes inactivity	13
H	Log all data extracts holding sensitive data and verify erased within 90 days	13
Appendix A	OMB Memorandum M-06-16	
B	NCUA Management Comments	

EXECUTIVE SUMMARY

The National Credit Union Administration (NCUA) Office of Inspector General (OIG) performed a limited scope review assessing the NCUA's actions to ensure that personally identifiable information (PII) and sensitive information is safeguarded, in accordance with the Office of Management and Budget (OMB) Memorandum M-06-16, *"Protection of Sensitive Agency Information."*[1]

To determine compliance with OMB M-06-16, we interviewed key agency officials responsible for privacy protection, reviewed applicable policies and procedures related to privacy, inquired about outstanding issues identified during the 2006 Federal Information Security Management Act (FISMA) audit, and compared encryption products used at NCUA with the National Institute of Standards and Technology's (NIST) Federal Information Processing Standards 140-2 validated product list. We performed limited tests on control procedures identified during this review.

As a result of this review, the OIG determined that NCUA needs to strengthen its privacy program to ensure that PII and sensitive data are appropriately protected. Most importantly, NCUA needs to ensure that member financial and personal data is protected from potential unauthorized access. Although we identified several weaknesses in the actions NCUA has taken to protect PII and sensitive information, we determined that NCUA is making progress to strengthen its policies and procedures for protecting both.

[1] http://www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf

INTRODUCTION:

Following numerous incidents at various Federal agencies involving the compromise or loss of sensitive personal information, OMB issued memorandum M-06-16 on June 23, 2006. That memorandum required agencies to take specific actions to protect PII and sensitive information as outlined in NIST Special Publication 800-53 and 800-53A. In addition, OMB recommended that agencies take four additional actions to protect sensitive agency information. OMB requested that agencies ensure that the safeguards outlined in M-06-16 be reviewed and in place within 45 days from the issuance of the memorandum (August 7, 2006). Inspectors General were also requested to conduct a subsequent review to asses their respective agency's compliance.

The President's Council on Integrity and Efficiency (PCIE) and Executive Council on Integrity and Efficiency (ECIE) jointly developed a data collection instrument (DCI) and review guide to assist Inspectors General in determining their agency's compliance with OMB Memorandum M-06-16. The review guide and DCI were closely linked to the actions OMB requested of agencies to protect PII and sensitive data and were likewise used to perform this limited scope review.

BACKGROUND:

PII is defined by OMB in M-06-19 as:

> "[*a*]*ny information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual."*[2]

Various statutes and authorities address the need to protect PII and other sensitive information held by government agencies, including the Federal Information Security Management Act (FISMA), the E-Government Act of 2002 (E-Gov Act), the Privacy Act of 1974, as amended, and OMB Circular A-130, *Management of Federal Information Resources*. In particular, FISMA requires agencies to have a security program and controls for systems to protect sensitive information.

FISMA also requires agencies to implement standards and guidelines developed by the NIST. Relevant standards are set forth in the following NIST publications:

[2] OMB Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, July 14, 2006

- Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004;

- FIPS Publication 200*, Minimum Security Requirements for Federal Information and Information Systems*, March 2006; and

- FIPS Publication 201*, Personal Identity Verification for Federal Employees and Contractors*, February 2005.

Additional guidance on protecting PII and other sensitive information is described in the NIST Special Publication (SP) 800 series. Among them, SP 800-53, *Recommended Security Controls for Federal Information Systems,* and SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems,* set forth key criteria for assessing compliance with FISMA requirements. This guidance forms the basis for the OMB M-06-16 Security Checklist covering protection of remote information. OMB Memorandum M-06-16 conveys OMB's intent that Federal agencies implement the checklist and take specific required actions for the protection of sensitive information to compensate for the lack of physical security controls when information is removed or accessed from outside the agency location.

OBJECTIVE:

The objective of this limited scope review was to assess the NCUA's actions to ensure PII and other sensitive information are safeguarded, in accordance with OMB Memorandum M-06-16, *"Protection of Sensitive Agency Information."*

SCOPE & METHODOLOGY:

To determine compliance with OMB M-06-16, we interviewed key agency officials responsible for privacy protection including the Senior Privacy Official, the Chief Information Officer, the Deputy Chief Information Officer, and the Senior Information Security Officer. We also reviewed applicable policies and procedures related to privacy, inquired about outstanding issues identified during the FISMA audit, and compared encryption products used at NCUA with NIST's FIPS 140-2 validated product list. We performed limited tests on control procedures identified during this review due to the limited time available to perform this review simultaneous with the annual FISMA audit. In addition, the NCUA was in the process of implementing many related procedures during and subsequent to our review which made it difficult to test during field work.

We conducted our work from August 8, 2006 through September 22, 2006. This report provides a snapshot of NCUA's progress in meeting OMB M-06-16 as of August 31, 2006.

This limited scope review was performed in accordance with the Quality Standards for Inspections issued by the PCIE/ECIE in January 2005.

RESULTS:

A. Confirm identification of PII and sensitive information protection needs

The NCUA needs to improve its process for identifying PII and sensitive information protection needs. For example, under the Privacy Act, NCUA identifies personal information it collects and maintains in its Systems of Records (SOR). However, during our review we identified some personal information maintained in NCUA's SOR that the agency did not, during the certification process, designate in the security categorization of "moderate," as we believe it should have been. While we found that NCUA's privacy related policies were outdated, we also learned that many were in the process of revision. We also determined that the agency did not specifically identify credit union member share and loan data obtained during a credit union examination as PII when, in our opinion, they should have been. We further confirmed that NCUA has not performed any Privacy Impact Assessments (PIA) for existing systems.

The NCUA Senior Privacy Officer is in the process of taking positive steps to address privacy responsibilities within the agency. For example, as mentioned above, at the time of this review the agency was in the process of revising both its SOR, which had not been updated since February 2000, as well as NCUA Instruction 3226.1, "Procedures for Implementing Provisions of the Privacy Act of 1974," which had not been revised since its issuance in 1976. In addition, the Senior Privacy Officer is considering proposing the issuance of a new agency instruction that specifically addresses information security. The Senior Privacy Officer also plans to perform a PIA for new agency identification cards and is considering whether additional PIAs are required. Finally, the Senior Privacy Officer has recommended to the Office of Human Resources (OHR) and the Office of the Chief Information Officer (OCIO) that an appropriate training program in privacy and information security for agency employees be devised and implemented.

We agree with the Senior Privacy Officer that credit union member data does not come within the definition of a SOR under the Privacy Act because the method of data retrieval is based on a charter number, not a member identifier. Nevertheless, we found that downloads obtained during a credit union examination contain PII as defined by OMB. Likewise, while NCUA has indicated that the AIRES downloads containing credit union member data require protection, it has not specifically developed a privacy policy articulating protections for this information. Credit union member data is vulnerable to unauthorized access or loss because it is stored in multiple formats in NCUA examiners' private homes across the country. Sensitive credit union member

data not identified as PII may not have adequate controls in place for its protection from unauthorized use. Consequently, the loss of this data could be used for identity theft.

NCUA has performed FIPS 199 categorizations of IT systems. However, there needs to be an improved process that compares information that may be identified in NCUA's SOR with the FIPS 199 categorizations to ensure that all PII and sensitive data are identified. For example, we identified PII in the Controller's Accounting System (CAS[3]) that were not ranked moderate. Although the overall confidentiality ranking for CAS was moderate, not all PII was identified within CAS as moderate. Some examples of PII not identified as requiring moderate protection includes names, SSN, account numbers, routing numbers, payment information, personnel information, etc. While certification and accreditation activities have been completed or are in process, a formal consideration of privacy has not occurred, resulting in some PII data not being identified during the categorization process which could result in inadequate controls over its protection.

Last year's FISMA evaluation noted that completion of the PIA was required as part of Certification and Accreditation (C&A) requirements. However, the NCUA has still not developed a PIA. NCUA needs to perform PIAs to ensure all PII data is accurately identified.

As shown in the excerpt from management's response to the 2006 FISMA audit report[4], NCUA opined that the trigger for developing PIAs has not yet occurred.

> "*Management acknowledges that the agency is subject to the requirement to prepare PIAs as provided in the E-Government Act. Management's view is that the requirement to prepare a PIA, required under the E-Government Act that became effective April 17, 2003, is triggered where an agency develops or procures an IT system or changes an existing system by adding new uses or new technologies or significantly changes how information in identifiable form is managed in the system. Generally, a PIA is required where a system change creates new privacy risks.*
>
> *NCUA last updated its Systems of Records notice effective in February 2000. See 65 Fed. Reg. 3486 (Jan. 21, 2000). Management's position is that, with the exception of the new Personnel Security and Identity Management Systems required under the Homeland Security Presidential Directive-12 (HSPD-12), the agency has neither developed nor procured new IT systems nor made a significant change to an existing system that created new privacy risks requiring preparation of a PIA. At this time, the agency is in the process of developing a PIA for these new systems, updating its Systems of Records notice, and preparing related notices and instructions for employees.*

[3] Examples of systems included in CAS are financial accounting, procurement, human resources, and travel systems.
[4] OIG Report to OMB on the National Credit Union Administration's Compliance with the Federal Information Security Management Act 2006, Report #OIG-06-06

Management maintains its view that it is not required to prepare and publish a PIA conforming to the requirements of the E-Government Act for IT systems in existence before April 2003 and which have been maintained without significant change. It is our position that our ongoing maintenance of these systems has not had an impact on the privacy risk of those systems. Routine maintenance does not change the basic functions of the programs; it normally entails updates to the user interface, revised edit formulas, etc., which have no bearing on the privacy risk level. Nevertheless, management acknowledges that a review of existing IT systems to ensure compliance with information privacy laws, regulation, and policy is an appropriate and commendable agency aspiration and intends to undertake such review as agency resources permit."

The E-Government Act guides agencies to:

"To conduct a PIA before: developing or procuring IT systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public or initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities or employees of the federal government). In general, PIAs are required to be performed and updated as necessary where a system change creates new privacy risks."

In response to management's comments to the FISMA Report, the OIG stated:

"*Per the requirements of section 208 of the E-Government Act of 2002, OMB issued guidance to agencies regarding the development of PIAs. The guidance provided by OMB applies to all executive branch departments and agencies. The Act requires agencies to conduct a PIA before developing or procuring IT systems that collect, maintain, or disseminate information in identifiable form from or about member of the public as well when the changes occur in information collection authorities, business processes or other factors affecting the collection and handling of such information. Since the inception of the E-Gov Act, NCUA has implemented several changes to business process and technical solutions that meet the above criteria as changes requiring an update or development of a PIA, including the distribution of external hard drives to store credit union audit data that are stored at the examiners' homes, an agency-wide update in operating systems (from 2000 to XP), distribution of new notebooks, and partial implementation of sensitive data encryption.*

It is the opinion of the OIG that any one of the above changes constitutes a change of the magnitude that requires the development of a PIA. Based on the identified changes to the methods of collecting, processing, and storing PII with the agency's IT infrastructure, NCUA should develop a PIA and maintain it on an ongoing basis."

Recommendations:

1. Update privacy related policies in accordance with the Privacy Act and applicable OMB guidance. Specifically, NCUA's Systems of Records notice has not been updated since Feb 2000 and the Privacy Instruction has not been updated since its issuance in 1976. The agency has indicated that it is in process of updating its SOR and the Privacy Instruction.

   Management Response: NCUA management issued a revised SOR on December 27, 2006.

   OIG Response: We agree with the action taken by NCUA.

2. Ensure that NCUA develops a more thorough policy addressing the protection of credit union member data obtained during credit union examinations. Specifically identify CU member data as sensitive PII as required by OMB.

   Management Response: NCUA management agreed to update and consolidate agency instructions.

   OIG Response: We agree with NCUA's planned actions.

3. Verify that all sensitive and PII data has been identified by performing PIAs on Moderate and High systems as required by NIST 800-53A and the E-Gov Act. Ensure that sensitive and PII data identified in the agency's SOR is compared with FIPS 199 categorizations and PIAs.

   Management Response: Although NCUA management disagrees, they "recognize that conducting PIAs is a worthwhile endeavor, which we intend to undertake, resources permitting."

   OIG Response: We maintain that under the E-Government Act of 2002, where OMB issued guidance to agencies regarding the development of PIAs; the guidance provided by OMB applies to all executive branch departments and agencies. The Act requires agencies to conduct a PIA before developing or procuring IT systems that collect, maintain, or disseminate information in identifiable form from or about member of the public as well when the changes occur in information collection authorities, business processes or other factors affecting the collection and handling of such information. However, we agree with the proposed actions by NCUA Management to undertake conducting PIAs.

B. Verify adequacy of organizational policy

NCUA's existing policy does not address information protection needs associated with PII that are accessed remotely or physically removed from agency premises. However, the Privacy Officer has stated that she is in the process of updating the policy which will incorporate information protection needs for PII accessed or stored remotely.

OMB M06-16 states, "*The policy should address the following specific questions:*

1. For Personally Identifiable Information physically removed:

a. Does the policy explicitly identify the rules for determining whether physical removal is allowed?

b. For personally identifiable information that can be removed, does the policy require the information be encrypted and that appropriate procedures, training, and accountability measures are in place to ensure that remote use of this encrypted information does not result in bypassing the protections provided by the encryption?

2. For Personally Identifiable Information accessed remotely:

a. Does the policy explicitly identify the rules for determining whether remote access is allowed?

b. When remote access is allowed, does the policy require that this access be accomplished via a virtual private network (VPN) connection established using agency-issued authentication certificate(s) or hardware token?

c. When remote access is allowed, does the policy identify the rules for determining whether download and remote storage of the information is allowed? (For example, the policy could permit remote access to a database, but prohibit downloading and local storage of that database.)"

Recommendation:

4. Identify PII and include information protection needs for PII accessed, transported, or stored remotely in agency privacy related policies.

   Management Response: NCUA management agrees.

   OIG Response: We agree.

C. Implement protections for PII transported/stored offsite

NCUA needs to improve protections for PII transported or stored offsite. We determined that NCUA is lacking a policy specific to PII transported or stored offsite.

During the FISMA audit, we identified PII and/or sensitive data that were not encrypted prior to being removed from agency premises. NCUA has started to implement some encryption capabilities, but did not consider NIST 140-2 validated products. We also observed during the FISMA audit that, with the exception of social security numbers, examiners do not have a specific awareness of their responsibilities to protect other PII and/or sensitive data.

NCUA is in the process of improving several controls related to remote storage. Specifically, the OIG identified sensitive credit union member data that was being stored remotely in an unencrypted format on notebooks, external hard drives, CDs, and personal USB drives during the FISMA audit. Subsequent to our review, the Office of the Chief Information Officer (OCIO) forced Windows XP encryption of selected folders on NCUA notebook computers and external hard drives.[5]

During NCUA's bi-annual regional conferences in August 2006, the OCIO began to distribute USB flash drives with encryption capability to examiners with instructions requiring their use for sensitive data, requiring remote storage, and limiting the use of CDs. However, we determined the USB drives purchased by NCUA are not 140-2 validated. (See section E for further discussion regarding this topic.) The OCIO also requested examiners to bring CDs containing sensitive data to the Regional Conference for destruction by heavy duty shredders provided by the OCIO.

Recommendation:

5. When updating agency polices and procedures, the agency should ensure that PII transported and/or stored offsite is specifically identified, including setting forth the steps needed to protect this data. In addition, incorporate encryption use in related security policies and procedures.

   Management Response: NCUA management agrees.

   OIG Response: We agree.

6. Increase employee awareness with respect to responsibility for protecting PII and other sensitive data.

   Management Response: NCUA management agrees.

   OIG Response: We agree

D. Implement protections for remote access to PII

NCUA has implemented some protections for remote access to PII such as establishing a VPN requiring smart cards. However, the agency needs to

[5] This control has not been tested by the OIG since it was in the process of being implemented during our review.

improve policies and procedures for protecting remote access to PII and sensitive data.

NCUA needs to specifically identify the types of PII that require remote access and the users authorized to remotely access PII. In addition, the policy and procedures should contain the actions required to protect PII that is accessed remotely.

NCUA established a VPN in 2000 requiring authentication using smart cards that are issued directly to each authorized user. Although the control requiring the smart cards was temporarily disabled for several months subsequent to our review, this control was reimplemented on October 12, 2006.

During the FISMA 2006 audit, the following related weaknesses were identified that could impact authorized access to PII and/or sensitive data:

- User account reconciliations are not performed to ensure appropriate authorized access
- Users can use unlimited password attempts to gain access to local data and users are not required to periodically change password.

Recommendation:

7. When updating agency policies, ensure that PII with remote access is specifically identified including what steps need to be taken to protect this data.

   Management Response: NCUA management agrees.

   OIG response: We agree

8. Implement recommendations identified during the FISMA audit related to privacy, such as performing user account reconciliations and tightening user password policies to ensure appropriate authorized access.

   Management Response: "The user account reconciliation has been completed. Existing password policies are appropriate."

   OIG response: We agree with the actions taken by NCUA.

E. Encrypt all data on mobile computers/devices

In M-06-16, OMB recommends that all agencies, "Encrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive, in writing…" In a recent presentation by NIST officials, NIST stated that

sensitive data should be classified Moderate or High triggering at least the moderate protection controls outlined in NIST 800-53A.

During the FISMA audit, the OIG identified several weaknesses where improvement was needed in enforcing the use of encryption of sensitive examination data. We identified sensitive data on examiner notebooks, external hard drives, CDs, and personal USB drives that were not encrypted. Subsequent to our FISMA audit and Privacy review, the OCIO has made some progress in protecting its sensitive data.

NCUA currently uses the following types of encryption:

- Windows XP on notebook computers,
- Windows XP on external hard drives,
- WinZip, and
- Lenovo flash drives.

After we initiated our Privacy review, the CIO sent several emails to users providing instructions on encryption. In addition, the OCIO began to force an encryption process that applied encryption to select folders and files located on notebook computers:

- D:\My Documents – every file and subfolder.
- D:\ncuaapps\aires32\exams - only the "exams" folder and its contents.
- D:\Outlook – every file and subfolder

Once the user initiated the encryption routine sent by the OCIO, the encryption would occur automatically in the background on a daily basis. When you place or create files or folders in encrypted folders, they are automatically encrypted. If you move a file or folder from an encrypted location to a non-encrypted location, the encryption will automatically be removed from the file or folder. In addition, if you move an encrypted file or folder to a CD or DVD, the encryption will automatically be removed. During our review, the OCIO also emailed instructions for encrypting the external hard drive with Windows XP.

Subsequent to our review, the OCIO implemented a technical solution that verified if certain folders and/or documents are encrypted. This solution forced the encryption on users that did not initiate the routine sent previously. If it finds documents not encrypted, it automatically encrypts the files without user intervention.

The OCIO provided WinZip to encrypt and password protect copies and/or backups of sensitive files. NCUA recommends to its examiners the use of 256 bit AES encryption with a minimum password 7 characters long and using three types of characters. The OCIO also began distribution of Lenovo flash drives to examiners during the regional conference.

Although the OCIO implemented and distributed WinZip and Lenovo flash drives for encryption, neither of these products have been FIPS 140-2 validated. FIPS 140-2 "… is applicable to all Federal agencies that use cryptographic-based security systems to protect sensitive information in computer and telecommunication Systems . . ." and provides a standard for Federal agencies when selecting cryptographic-based security systems for protecting sensitive data. FIPS 140-2 validation provides assurance because products have been independently tested to ensure they meet applicable standards. The following is an excerpt from NIST explaining their position on unvalidated cryptography modules:

> **"Use of Unvalidated Cryptographic Modules by Federal Agencies and Departments**
>
> FIPS 140-2 precludes the use of unvalidated cryptography **for the cryptographic protection** of sensitive or valuable data within Federal systems. Unvalidated cryptography is viewed by NIST as providing **no protection** to the information or data – in effect the data would be considered unprotected plaintext. **If the agency specifies that the information or data be cryptographically protected**, then FIPS 140-2 is applicable. In essence, if cryptography is required, then it must be validated. "[6]

Recommendation:

9. Ensure any encryption products implemented or considered for implementation comply with applicable laws and regulations, including FIPS 140-2.

   Management Response: "In the future, to the extent that we can find NIST-certified products that meet our quality and performance requirements as well as our schedule demands, we will ensure, to the best of our ability, that we purchase certified products."

   OIG Response: We agree with the intent of NCUA's proposed action to purchase certified products.

10. Update security policies and procedures with encryption instructions, user responsibilities, and prohibit use of CDs, personal USB drives, and other unencrypted media for storage of sensitive and/or PII data.

    Management Response: NCUA management agreed.

    OIG Response: We agree.

[6] http://csrc.nist.gov/cryptval/

F. Allow remote access only with two-factor authentication

At the time of our review, smart cards were not required for authentication to the VPN because they were temporarily disabled as a result of expired certificates. Effective October 12, 2006, the OCIO reimplemented smart card authentication for the SWAP VPN.

G. Use a time-out after 30 minutes inactivity

We determined that some remote access and mobile devices used by the NCUA are configured to require reauthentication after 30 minutes of inactivity. Notebook computers used by NCUA personnel are configured to time-out after 30 minutes of inactivity. However, we determined that Blackberry devices time-out settings can be controlled by the user. We also noted that applications used by the NCUA do not have a time-out feature.

Recommendation:

11. When Blackberry devices are issued, ensure they are configured so reauthentication is required after 30 minutes of inactivity. In addition, determine if the configuration can be locked down to prevent users from changing the configuration.

    Management Response: NCUA management implemented this recommendation.

    OIG Response: We agree with the actions taken by NCUA.

H. Log all data extracts holding sensitive data and verify erased within 90 days

The OIG recognizes the difficulty associated with this control and agrees that if the resources exceed the benefits provided by this control and the agency has implemented related controls contained in SP 800-53, SP800-53A, and OMB 06-16, sufficient protection would exist that would make this control redundant of better controls.

Appendix A

http://www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf

Appendix B

TO: James Hagen, Assistant Inspector General for Audits

FROM: Sheila A Albin, Associate General Counsel & Senior Agency Privacy Official
Neil McNamara, Deputy Chief Information Officer

SUBJ: Comments on OIG's Review of NCUA Compliance with OMB M-06-16

DATE: January 30, 2007

Introduction and Summary

This memorandum responds to the OIG's request, dated January 22nd, for management's comments on its Draft Review of NCUA Compliance with OMB M-06-16 (Draft Review).

We generally support the recommendations in the Draft Review but, as discussed more specifically below, management disagrees with or believes several of the eleven recommendations require clarification. Several recommended actions were already underway at the time of OIG's review in August 8 to September 22, 2006, and, as noted below, some were completed before the first Draft Review was provided to management.

This memorandum also provides the following comments to clarify or correct certain premises and other statements in the Draft Review forming the bases for the recommendations.

Discussion

For ease of reference, these particular comments track the order in which the subject or a statement appears in the Draft Review, not necessarily in order of significance.

Page 1 and throughout. *"Personally Identifiable Information"*

Use of the phrase "personally identifiable information" (PII) understandably creates some confusion because the definition used, which is the only one management believes OMB has provided, is applied to other legal requirements. The definition of PII quoted at page 2 of the Draft Review is an OMB definition in OMB M-06-19 that, as defined in that memorandum, applies to OMB's policy on reporting security incidents. This memorandum followed previous OMB issuances on information security, including OMB M-06-16, the subject of the Draft Review. Although using this definition in considering compliance with OMB M-06-19 is not objectionable, we note that OMB M-06-19, itself, does not define PII.

PII is not the same and should not be equated with the definition of a privacy record under the Privacy Act. Also, PII is not defined in FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems." FIPS 199, in fact, has a broader purpose stated as "information security," not only information about individuals.[7]

The second Draft Review now generally references PII and sensitive information together. Nevertheless, coupling the categories does not address the lack of clarity.

At page 5, the Draft Review notes the Privacy Officer is developing a plan for privacy and information security training. To clarify, the Privacy Officer met with representatives of OHR and OCIO in 2006 to address training and revision of existing agency instructions on privacy and information security. It is, however, the Director of OHR, with "advice from the General Counsel," who is responsible for Privacy Act training. 12 C.F.R. §792.69. In December 2006, OHR provided the Privacy Officer an outline of its plans to address Privacy Act training. The Privacy Officer anticipates OHR and OCIO staff will work together to develop appropriate training in information security for agency employees.

We recommend the Draft Review note in some fashion (possibly a footnote on page 5 and to recommendation #1) that the SOR has been updated, published in the Federal Register, and posted on the agency's website.

At page 6, the Draft Review states, in connection with noting that NCUA has performed FIPS 199 categorizations of IT systems, that "there needs to be an improved process that compares information that may be identified in NCUA's SOR [Privacy Act Systems of Records Notice] wiith the FIPS 199 categorizations to ensure that all PII and sensitive data are identified." This statement is not clear but appears to state the current FIPS 199 categorization is inadequate in that it does not identify all PII and, further, that reviewing the systems of records identified in NCUA's Privacy Act notice would be helpful.

While review of NCUA's SOR Notice may be helpful in reviewing the agency's FIPS 199 categorization, we note that, both legally and operationally, the agency's responsibilities and requirements for information security and Privacy Act compliance are different.

OIG Recommendations

1. Update privacy related policies in accordance with the Privacy Act, FOIA, and applicable OMB guidance. Specifically, NCUA's Systems of Records notice has

[7] FIPS 199 requires categorization of information and information systems as having low, moderate, or high levels of risk in terms of the security objectives of confidentiality, integrity, and availability. It gives examples of types of information that should be categorized, such as "privacy," but does not define types of information.

not been updated since Feb 2000 and the Privacy Instruction has not been updated since its issuance in 1976. The agency has indicated that it is in process of updating its SOR and the Privacy Instruction.

Comment: Reference to FOIA is inappropriate as noted above and a revised Systems of Records Notice has now been issued. 71 Fed. Reg. 77807 (Dec. 27, 2006).

2. Ensure that NCUA develops a policy addressing the protection of credit union member data obtained during credit union examinations. Specifically identify CU member data as sensitive PII as required by OMB.

   Comment: NCUA already has several agency Instructions setting out agency policy on information security, including the protection of sensitive credit union data obtained in the examination process, for example, NCUA Instructions 13500.2, 13500.05, and 13500.06. OCIO acknowledges agency policy can be improved and intends to update and consolidate several of these Instructions to address information security, including more specific direction to employees on safeguarding PII obtained in the credit union examination process.

3. Verify that all sensitive and PII data has been identified by performing PIAs on Moderate and High systems as required by NIST 800-53A and the E-Gov Act and comparing sensitive and PII data identified in the SOR, data that may be subject to withholding based on FOIA exemptions, FIPS 199 categorization, and PIAs.

Comment: The Draft Review discusses the necessity of performing privacy impact assessments (PIAs) and notes the key criterion for determining if a PIA is required is "where a system change creates new privacy risks." Quoting from OIG's response to management's comments on OIG 2006 Report to OMB on the NCUA's Compliance with FISMA, the Draft Review states on page 7:

> *Since the inception of the E-Gov Act, NCUA has implemented several changes to business process and technical solutions that meet the above criteria* [a system change creates a new risk] *as changes requiring an update or development of a PIA, including the distribution of external hard drives to store credit union audit data that are stored at the examiners' homes, an agency-wide update in operating systems (from 2000 to XP), distribution of new notebooks, and partial implementation of sensitive data encryption.*
>
> *It is the opinion of the OIG that any one of the above changes constitutes a change of the magnitude that requires the development of a PIA.*

Management's view is the specifically cited examples did not create new risks. To the contrary, three of the changes actually *decreased* the privacy risk, while the fourth had no impact on risk:

- The external hard drives issued to field staff automatically encrypt the data stored on them. They replace the unencrypted media previously used by examiners for data backup, such as CD-ROMs and flash drives, thereby reducing privacy risk.
- The Windows XP operating system is inherently more secure than Windows 2000; converting to Windows XP therefore decreased the security and privacy risks to NCUA data.
- The distribution of newer, better notebooks to replace the old notebooks had no impact on privacy risks.
- Implementation of encryption of sensitive data obviously decreases the privacy risk.

At pages 6-7, the Draft Review quotes management's previous response to the 2006 FISMA audit report. In brief, to avoid repetition, management's view continues to be that PIAs are not required for systems in existence before April 2003 unless alteration to so-called legacy systems create new risks. The Draft Review correctly notes at page 5 that PIAs for new systems will be developed.

The core of management's disagreement with OIG may be over the meaning of the word "system" and the criterion that there is an increase in risk.

As noted by OIG, NCUA has indeed conducted several procurements in recent years, including the current notebook computers and the external hard drives for field staff. OCIO's view is these were procurements of hardware, not systems. Our view is the word system generally means a software application that collects, processes, or produces data, including the PII that is at the heart of the discussion regarding PIAs.

When NCUA replaced the notebook computers, the *systems* that process PII were all migrated from the old hardware platform to the new hardware platform. The *systems* were not changed.

Nonetheless, as we have acknowledged previously, we recognize that conducting PIAs is a worthwhile endeavor, which we intend to undertake, resources permitting.

4. Identify PII and include information protection needs for PII accessed, transported, or stored remotely in agency privacy related policies.

   Comment: Generally agree.

5. When updating agency polices and procedures, the agency should ensure that PII transported and/or stored offsite is specifically identified, including setting forth

the steps needed to protect this data. In addition, incorporate encryption use in related security policies and procedures.

Comment: Generally agree.

6. Increase employee awareness with respect to responsibility for protecting PII and other sensitive data.

   Comment: Generally agree.

7. When updating agency policies, ensure that PII with remote access is specifically identified including what steps need to be taken to protect this data.

   Comment: Generally agree.

8. Implement recommendations identified during the FISMA audit related to privacy, such as performing user account reconciliations and tightening user password policies to ensure appropriate authorized access.

   Comment: The user account reconciliation has been completed. Existing password policies are appropriate.

9. Ensure any encryption products implemented or considered for implementation comply with applicable laws and regulations, including FIPS 140-2.

   Comment: When NCUA purchased encrypted flash drives for all field staff, several constraints drove the selection. We needed a high quality product that used the NIST standard encryption technology, worked with our existing equipment, and was available in time for distribution at the Regional Conferences. It should be noted that NCUA had a very narrow window of time between receipt of OMB memo M-06-16 (dated June 23, 2006) and the NCUA Regional Conferences held two months later.

   We purchased sample drives from Lenovo, the manufacturer of our notebooks, and Kingston, one of the industry leaders in high quality storage. The Kingston product requires users to have administrative privileges, which made it unusable in our environment. The Lenovo device required administrative privileges to install on the machine, but not to use it, which is why we chose the device we did.

   In the future, to the extent that we can find NIST-certified products that meet our quality and performance requirements as well as our schedule demands, we will ensure, to the best of our ability, that we purchase certified products.

10. Update security policies and procedures with encryption instructions, user responsibilities, and prohibit use of CDs, personal USB drives, and other unencrypted media for storage of sensitive and/or PII data.

Comment: Generally agree.

11. When Blackberry devices are issued, ensure they are configured so reauthentication is required after 30 minutes of inactivity. In addition, determine if the configuration can be locked down to prevent users from changing the configuration.

    Comment: This recommendation has been implemented.

Conclusion

Thank you for the opportunity to comment. If you believe it would be helpful to discuss any of the comments before issuing your final Review, we are available to meet or discuss them with your staff.