NATIONAL CREDIT UNION ADMINISTRATION
OFFICE OF INSPECTOR GENERAL

FOLLOW-UP REVIEW
OF
NCUA ENCRYPTION

Report #OIG-07-11 November 15, 2007

William A. DeSarno
Inspector General

Released by:

James Hagen
Asst IG for Audits

Auditor-in-Charge:

W. Marvin Stith, CISA
Sr Information Technology Auditor

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The National Credit Union Administration (NCUA) Office of Inspector General (OIG) performed an audit to determine if NCUA is adequately protecting sensitive electronic data. To determine whether the NCUA adequately protects sensitive electronic data, we interviewed a judgmental sample of examiners and reviewed the examiners' computer equipment[1]. We also interviewed the Chief Information Officer and reviewed policies and procedures related to protecting sensitive data.

We determined that the NCUA is adequately protecting sensitive electronic data. The examiners were primarily saving exam-related files to their encrypted 'My Documents' folder as advised by the OCIO. In addition, we did not identify any unencrypted exam files on the NCUA-issued external hard drives. However, we determined the NCUA could make improvements to better protect this data. Specifically, while 94 percent of the exam files we identified on the laptops we reviewed were encrypted, some examiners had potentially sensitive unencrypted credit union data on their computer equipment. In addition, there was unrestricted access to sensitive credit union data on the NCUA intranet. We also learned that while the encryption technology the NCUA used adequately protected sensitive data if used as guided, the NCUA OCIO was planning to implement a strategy to better protect electronic PII and other sensitive data.

Our report includes five recommendations to NCUA to improve the security, access and storage of sensitive credit union data. Management agreed with all five recommendations and has started corrective action.

[1] Computer equipment includes NCUA-issued laptops, external hard drives, and USB flash drives, and unencrypted media such as USB flash drives and CDs.

BACKGROUND:
In today's computing environment, there are many threats to the confidentiality of information stored on end user devices, which could cause information stored on the devices to be accessed by unauthorized parties. Some threats are unintentional, such as human error, while others are intentional. These threats are posed by people with many different motivations, including causing mischief and disruption and committing identity theft and other fraud. One common threat against end user devices is loss or theft. Someone with physical access to a device has many options for attempting to view the information stored on the device. This is also a concern for insider attacks. To prevent disclosures of PII and other sensitive data, the information needs to be secured.

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. The memorandum required agencies to take specific actions to protect PII and sensitive information as outlined in NIST Special Publication (SP) 800-53 and 800-53A. In addition, OMB recommended that agencies take 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 assess their respective agency's compliance. The OIG issued a report in February 2007 (OIG-07-01) and determined the NCUA needed to improve protections for PII transported or stored offsite. During this Privacy review we addressed PII or sensitive data we identified during the FY 2006 FISMA audit that were not encrypted prior to being removed from agency premises.

Before we completed the Privacy review, the NCUA had started to implement some encryption capabilities. The CIO sent several emails to users providing instructions on encryption. In addition, the OCIO began to distribute an encryption process that applied encryption to select folders and files located on agency laptops. 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. Subsequent to the Privacy review, the OCIO implemented a technical solution that verified if certain folders or documents were encrypted. This solution forced the encryption on users that did not initiate the routine sent previously. If the routine identified unencrypted documents, it automatically encrypted the files without user intervention.

OBJECTIVE:

The objective of this review was to determine if NCUA is adequately protecting sensitive electronic data.

SCOPE & METHODOLOGY:

To determine whether the NCUA adequately protected sensitive electronic data, we interviewed a judgmental sample of examiners and reviewed the examiners' computer equipment. We searched the examiners' computer equipment using the following criteria to identify exam-related files:

exam.* - to identify exam files that contained *'exam'* in the document title

- *share*.* - to identify exam files that contained *'share'* in the document title
- *loan*.* - to identify exam files that contained *'loan'* in the document title
- *.nb7 - to identify backup files[2]

Some of the common exam files and some unique exam files we identified contained sensitive credit union data. For example, we determined that one of the common exam files entitled '*Query Report Shares Greater Than $100,000.*doc' contained credit union member names and account numbers. However, we did not view the contents of this file type each time we found it unencrypted on an examiner's computer equipment. Instead, we assumed that exam files with the same common filenames *potentially* contained the same type of sensitive data. On the other hand, we did view the contents of the other unencrypted unique files we identified to determine that they contained sensitive data. We also interviewed the Chief Information Officer and reviewed policies and procedures related to protecting sensitive data.

We conducted our fieldwork from April 2007 through November 2007 and performed this review in accordance with Generally Accepted Government Auditing Standards.

[2] Backup files with this extension were created by the NovaStor NovaBACKUP software, which the NCUA used previously for backups. The NCUA uses a new procedure and software that restricts backups to the NCUA-issued encrypted external hard drives.

RESULTS:

A. Sensitive credit union data is unprotected on some examiners' computer equipment.

Examiners are primarily encrypting exam-related files; however, we identified unencrypted exam files on some of the examiners' laptops, NCUA-issued USB flash drives, and unencrypted USB flash drives. Some of these files potentially contained sensitive credit union data such as credit union member names and account numbers; CAMEL ratings; and credit union operating exceptions, violations of law or regulation, or unsound policies, practices or procedures. Following are the results of our review of the examiners' computer equipment:

- Nine of the fifteen examiners we interviewed had a total of 214 unencrypted exam files located on their C: drive. We determined that (107) of these unencrypted files potentially contained sensitive data. We were able to determine that 64 of these sensitive files[3] were located either in the Desktop folder, Desktop\OldDesktop folder or a Desktop*%Other folder*%\[4]. In addition, were able to determine the dates of the 107 sensitive files as follows:

Dates	2005 and Earlier	Jan 1, 2006 – Aug 31, 2006[5]	Sep 1, 2006 – Dec 31, 2006	2007	Total
Files	47	16	10	34	**107**

Table A. Dates of Potentially Sensitive Exam Files

  - Between October and November 2005 the OCIO created an *OldDesktop sub* folder within the laptops' *Desktop* folder to store files that existed on users' desktops prior to the NCUA's transition to a new operating system. In February 2006 the NCUA OCIO advised field staff to delete old exam files before the agency-wide conversion to new laptops. Some examiners may have forgotten about the exam files placed in their *OldDesktop* folders in 2005.

  - The NCUA OCIO 2006 IT policy (2006 Hi-Tech Manual) provided users guidance on encrypting folders; however, it did not mandate that users encrypt folders or advise which folders to encrypt. In addition, when the OCIO implemented its new encryption procedures in August 2006, it did not advise field staff to delete old exam files or move exam files still needed to the encrypted folders. This lack of guidance may

[3] We were unable to identify the locations of the other 43 files containing sensitive information.
[4] *%OtherFolder%* substitutes for the name of any subfolder of the Desktop folder other than the OldDesktop folder.
[5] The NCUA OCIO forced the encryption policy effective September 1, 2006.

have contributed to why some exam files existed in other unencrypted folders on examiners' laptops.

- The NCUA OCIO 2007 IT policy (2007 Hi-Tech Manual) advised that all work-related files be put into the encrypted 'My Documents' folder[6] and that no confidential information should be saved on the desktop. A few examiners admitted they saved exam files to the desktop, but also said they later deleted them. Regardless, some examiners did not follow NCUA policy.

- We identified 51 unencrypted files on three NCUA-issued USB flash drives.[7] More than half of these files potentially contained sensitive credit union data. In addition, three examiners said they used unencrypted USB flash drives to save exam files. However, we did not identify any remaining unencrypted files on these drives. The NCUA previously authorized examiners to purchase other computer media such as USB drives and CDs. The NCUA did not have a formal policy requiring examiners to use the NCUA-issued USB flash drive.[8] However, in August 2006, the OCIO instructed examiners to use the NCUA-issued USB flash drives for sensitive data.[9] Some examiners did not follow OCIO guidance.

- We reviewed external hard drives that examiners used for backing up files on their laptops. All the files on the external hard drives were encrypted. However, six of the 15 examiners had old unencrypted backup files[10] on their laptops and a CD. The NCUA OCIO 2006 IT policy provided instructions to examiners to backup files weekly to their external hard drives using NovaStor NovaBACKUP software. The NCUA used the NovaBACKUP software prior to when the NCUA implemented its new encryption policies and procedures. Therefore, these backup files may have contained unencrypted exam files. In addition, the 2006 IT policy indicated examiners could use other computer media such as CDs for more frequent backups. However, in August 2006 the OCIO provided instructions to examiners to limit the use of CDs and requested examiners take their CDs to the regional conference to be destroyed.[11] Some examiners did not follow the OCIO's guidance on backing up files to external hard drives and other computer media or for destroying CDs.

---

[6] The 'My Documents' folder is located on the D: drive.

[7] The OCIO distributed USB flash drives with an encryption capability to examiners beginning during the NCUA regional conference in August 2006. The USB flash drive's encryption capability is not automatic. It requires the user to login to the feature in order to place files in the encrypted portion of the drive; otherwise, any files a user places on the drive are unencrypted.

[8] In the OIG report, Review of NCUA's Compliance with OMB M-06-16 Protection of Sensitive Agency Information (Report #OIG-07-01) dated February 7, 2007, the OCIO agreed to develop a policy that addresses information protection needs for PII accessed, transported, or stored remotely.

[9] The NCUA is developing an agency instruction that requires examiners to use computer equipment that is encryption-capable with the encryption function enabled.

[10] These were the backup files with the *.nb7 extension* created using the NovaStor NovaBACKUP software.

[11] The NCUA is developing a policy that does not allow the use of unencrypted computer equipment.

- We identified two NCUA-issued USB flash drives on which the encryption login feature did not function. One of these drives contained unencrypted files as discussed above. We previously reported these drives were not NIST-validated and therefore were not approved for use by NIST. The OCIO agreed to purchase new drives if possible and planned to distribute NIST-validated drives in January 2008.

If examiners' laptops or other media are lost or stolen, sensitive credit union data could be exposed to unauthorized third parties potentially resulting in the theft of credit union members' identities, causing embarrassment to the NCUA and exposing the agency to potential liabilities and potentially exposing the NCUA to liabilities.

Recommendations #1: NCUA OCIO should reiterate to examiners the requirement to save all exam-related files only to the encrypted 'My Documents' folder and to use only NCUA-issued USB flash drives for exams or interim backups.

Management Response: Agreed. CIO Verner will issue this reminder to all field staff.

OIG Response: We agree with proposed action.

Recommendations #2: NCUA OCIO should require examiners to delete unencrypted exam files that are not needed and to delete old backup files from their computer equipment or if needed, to move the files to the encrypted "My Documents" folder.

Management Response: Agreed. CIO Verner will include this in his reminder message to staff.

OIG Response: We agree with proposed action.

Recommendations #3: NCUA OCIO should assist examiners in locating unencrypted exam and backup files and require the examiners to move or delete these files.

Management Response: Agreed. CIO Verner will include this in his reminder message to staff.

OIG Response: We agree with proposed action.

Recommendations #4: Until the NCUA OCIO is able to issue NIST-validated USB flash drives, OCIO should investigate and resolve problems with the operation of the encryption software on the current NCUA-issued drives.

Management Response: Agreed. CIO Verner will include this in his reminder message to staff.

OIG Response: We agree with proposed action.

B. Sensitive credit union data is exposed on the NCUA's intranet

The NCUA maintains a link to credit union exam data (AIRES Downloads) on its intranet. Exam data is available for credit unions in all five NCUA regions. The AIRES Downloads repository contains the same type of files examiners maintain on their laptops and contains files at least as far back as 2000. Therefore, these files also potentially contained sensitive credit union data such as credit union member names and account numbers; CAMEL ratings; and credit union operating exceptions, violations of law or regulation, or unsound policies, practices or procedures. For example, a file we downloaded for one credit union contained a subset of the credit union's member names, social security numbers and credit card numbers. There are no restrictions to limit or control access to this data. Consequently, anyone with access to the NCUA intranet can access this data regardless of whether exam data is within the scope of their responsibilities. For example, any examiner from any region could access exam data for any credit union within their region or any other region. Also, an NCUA employee who works in a non-exam area could access exam data for credit unions in any of the five regions. These users would be able to view and save sensitive credit union data.

OMB A-130, Appendix III indicates that the greatest harm to a system has come from authorized individuals engaged in improper activities, whether intentional or accidental. In addition, OMB Memorandum 07-16 indicates that limiting access to PII to only those individuals who must have such access may be one way to greatly reduce the risks related to a data breach of PII. The Privacy Act of 1974 requires agencies to establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual on whom information is maintained.

Uncontrolled access to the AIRES exam data by NCUA users without a need-to-know could result in the misuse of sensitive credit union data, the theft of credit union members' identities, cause embarrassment to the NCUA and expose the agency to potential liabilities.

Recommendation #5: NCUA OCIO should implement technical access controls to AIRES exam data on the NCUA intranet.

Management Response: Agreed. OCIO will work with E&I to establish and implement both procedural guidance and technical controls that improve the security of data located on the NCUA Intranet site. Options we are exploring include:

- Migrating sensitive data to from the intranet to SharePoint where permissions for accessing the information is more easily defined;
- Developing a log to identify users who download sensitive data from the intranet; and/or,
- Archiving additional sensitive data so it is not as accessible as the current location.

OIG Response: We agree with proposed action.

Other Audit Matters – Encryption Technology

The NCUA implemented an adequate encryption technology to protect sensitive credit union data. However, as discussed above, some sensitive exam data is still exposed on NCUA computer equipment.

NIST Draft SP 800-111 indicates there are many technologies available for encrypting data stored on end user devices. Encryption can be applied to individual files containing sensitive information, or broadly, such as encrypting all storage. Three of the most commonly used technologies are full disk encryption, virtual disk encryption and volume encryption, and file/folder encryption:

1. *Full disk encryption (FDE)* is the process of encrypting all the data on the hard drive used to boot a computer, including the computer's operating system (OS), and permitting access to the data only after successful authentication to the FDE product. For a computer that is not booted, all the information encrypted by FDE is protected, assuming that pre-boot authentication is required.

2. *Virtual disk*[12] *encryption* is the process of encrypting a container, which can hold many files and folders, and permitting access to the data within the container only after proper authentication. *Volume*[13] *encryption* is the process

[12] A virtual disk is a program that simulates a hard disk drive, using part of the computer's random access memory. Files can be copied into the virtual disk and edited. The virtual disk cannot store files permanently; the updates must be written to the hard disk or floppy disk before the power is turned off.

[13] A volume is a fixed amount of storage on a disk or tape. The term *volume* is often used as a synonym for the storage medium itself, but it is possible for a single disk to contain more than one volume or for a volume to span more than one disk.

of encrypting an entire volume and permitting access to the data on the volume only after proper authentication.

3. *File encryption* is the process of encrypting individual files on a storage medium and permitting access to the encrypted data only after proper authentication. *Folder encryption* is very similar to file encryption, only it addresses individual folders instead of files.

The NCUA uses file encryption technology, specifically Windows Encrypting File System (EFS)[14]. This encryption is selective and encrypts files automatically, based on defined attributes like file location (e.g., folder), file type (e.g., spreadsheets) or source application (e.g., all Excel files). The NCUA provides encryptions of files based on their location in folders the OCIO specified. EFS relies on sensitive data being written into these protected locations and cannot stop users from copying encrypted files to unencrypted locations, which is what has occurred within the NCUA.

The CIO informed us the OCIO plans to implement a new strategy for encryption, data security and PII that includes:

- NIST-approved USB flash drives the OCIO plans to issue in January 2008
- Email encryption
- Full disk encryption
- A new software product to encrypt removable media
- Software to protect file permissions (e.g., encryption) as the data moves from one place to the next.

We believe the CIO's strategy will result in improved encryption and data security that will better protect the NCUA's PII and other sensitive data. We will follow the OCIO's efforts to improve the protection of the agency's PII and sensitive data.

[14] Windows EFS is Microsoft's basic file/folder encryption tool.

APPENDIX

NCUA MANAGEMENT COMMENTS

OCIO/D2V/NRM:nrm

To: Inspector General Bill DeSarno

From: Executive Director J. Leonard Skiles /S/

Subject: Comments on OIG Review of NCUA Encryption

Date: November 13, 2007

We have reviewed your draft report on data encryption and found it to be very thorough and informative. We agree with your findings. OCIO and E&I will work together to implement them.

The first four recommendations pertain to sensitive credit union data found on examiners' hard drives:

1. NCUA OCIO should reiterate to examiners the requirement to save all exam-related files only to the encrypted 'My Documents' folder and to use only NCUA-issued USB flash drives for exams or interim backups.

   Management Response: Agreed. CIO Verner will issue this reminder to all field staff.

2. NCUA OCIO should require examiners to delete unencrypted exam files that are not needed and to delete old backup files from their computer equipment or if needed, to move the files to the encrypted "My Documents" folder.

   Management Response: Agreed. CIO Verner will include this in his reminder message to staff.

3. NCUA OCIO should assist examiners in locating unencrypted exam and backup files and require the examiners to move or delete these files.

   Management Response: Agreed. CIO Verner will include this in his reminder message to staff.

4. Until the NCUA OCIO is able to issue NIST-validated USB flash drives, OCIO should investigate and resolve problems with the operation of the encryption software on the current NCUA-issued drives.

   Management Response: Agreed. CIO Verner will include this in his reminder message to staff.

The final recommendation pertains to sensitive credit union data accessed via the NCUA Intranet:

- NCUA OCIO should implement technical access controls to AIRES exam data on the NCUA intranet.

  Management Response: Agreed. OCIO will work with E&I to establish and implement both procedural guidance and technical controls that improve the security of data located on the NCUA Intranet site. Options we are exploring include:

  - Migrating sensitive data to from the intranet to SharePoint where permissions for accessing the information is more easily defined;

  - Developing a log to identify users who download sensitive data from the intranet; and/or,

  - Archiving additional sensitive data so it is not as accessible as the current location.

Thank you for giving us the opportunity to review the draft report. If you have any questions about our response, please feel free to call Doug Verner.

cc: Director David Marquis
Director Doug Verner
Assistant IG Jim Hagen
Acting-DED Dave Hibshman