OFFICE OF INSPECTOR GENERAL

NCUA
National Credit Union Administration

AUDIT OF NATIONAL CREDIT UNION ADMINISTRATION'S MEASURES TO PROTECT ELECTRONIC CREDIT UNION MEMBER INFORMATION DURING THE EXAMINATION PROCESS

REPORT #OIG-15-09
JUNE 8, 2015

James W. Hagen
Inspector General

Released by:

R. William Bruns
Deputy Inspector General

W. Marvin Stith, CISA, CICA
Sr. Information Technology Auditor

TABLE OF CONTENTS

ACRONYMS AND ABBREVIATIONS

AES	Advanced Encryption Standard
AIRES	Automated Integrated Regulatory Examination System
E&I	NCUA Office of Examination and Insurance
External Data Protection Policy	NCUA Instruction 13500.09, Security of External Party's Documentation (March 25, 2008)
FIPS	Federal Information Processing Standard
NCUA	National Credit Union Administration
NCUA Communications Manual	NCUA Communications Manual – Procedures and Requirements for NCUA Communications Products (Revised December 2014)
NCUA email Policy	NCUA Instruction 13302.1 (REV), Electronic Mail, Communications, and Filing/Storage of Electronic Documents (April 1, 1996)
NCUA Handbook	NCUA Information Security Policy (Version 1.6, July 8, 2014)
NCUA Rule	12 Code of Federal Regulations, Part 748
NCUA Rules document	NCUA Rules of Behavior
NIST	National Institute of Standards and Technology
OCIO	NCUA Office of the Chief Information Officer
OIG	NCUA Office of Inspector General
ONES	NCUA Office of National Examination and Supervision
OSCUI	NCUA Office of Small Credit Union Initiatives
PII	Personally Identifiable Information
PSFCU	Palms Springs Federal Credit Union
Security Training	NCUA Security Awareness Training
[redacted]	[redacted]

EXECUTIVE SUMMARY

We conducted an audit to determine whether NCUA has adequate controls in place to protect sensitive, confidential, or personally identifiable electronic credit union information during examinations.

We initiated this audit as a result of the incident involving the breach of Palm Springs Federal Credit Union member information that occurred on October 20, 2014. To accomplish this audit, we conducted fieldwork at NCUA's headquarters in Alexandria, Virginia and with NCUA Regional office management and staff via the NCUA email system. We interviewed management and staff from the Office of the Chief Information Office (OCIO), the Office of Examination and Insurance (E&I), the Office of National Examinations and Supervision (ONES), the Office of Small Credit Union Initiatives (OSCUI), and Regional offices. We reviewed NCUA regulation, policies, procedures and training associated with protecting sensitive, confidential, or personally identifiable information.

We determined that NCUA has provided examiners with appropriate tools with which to securely receive electronic information from credit unions during the examination process. However, we also determined:

1. NCUA does not require credit unions to provide sensitive, confidential, and personally identifiable credit union member information to NCUA staff in a protected manner.

2. NCUA needs to improve its policies, procedures and training to help ensure NCUA staff take appropriate measures to protect sensitive, confidential, and personally identifiable electronic credit union member information during examinations; and

3. NCUA needs to improve its guidance to require NCUA staff to use specific tools to transfer sensitive, confidential, and personally identifiable electronic credit union member information during examinations.

We made seven recommendations to NCUA management to help increase staff awareness regarding the importance of protecting sensitive credit union member information and to ultimately strengthen the agency's efforts to protect this information in its electronic format.

We appreciate the cooperation and courtesies NCUA management and staff provided to us during this review.

BACKGROUND

General Information

The National Credit Union Administration (NCUA) defines a breach as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons, other than authorized users, and for an other than authorized purpose, have access or potential access to personally identifiable information, whether physical or electronic. In addition, NCUA defines terms related to private information as follows:

- Confidential Information - Any information which by itself, or in combination with other information, could be used to cause harm to a credit union, credit union member, or any other party external to NCUA.

- Personally Identifiable Information (PII) - Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date of birth and biometric records.

- Sensitive Information - Any information concerning a person or their account which is not public information, including any nonpublic PII.

Palm Springs Federal Credit Union[1] Incident Information

On October 20, 2014 during an examination of Palm Springs Federal Credit Union[2] (PSFCU), there was a breach of PFSCU sensitive and personally identifiable member information. Specifically, during the examination, a PSFCU manager provided an unencrypted flash drive containing PSFCU member information to NCUA examiners who were operating out of a common room of the city-operated building where PSFCU is located. The examiners left the flash drive exposed on a table within this room, which anyone authorized to be in the building had access to. When the PSFCU manager later requested that the examiners return the flash drive, the examiners could not locate it. Staff from NCUA and PSFCU were unsuccessful in their efforts to locate the flash drive.

NCUA determined the flash drive contained the names, addresses, social security numbers, and account numbers belonging to PSFCU members. NCUA also determined, however, that the data did not include member passwords or PINs. NCUA concluded that the examiners failed to exercise proper care over the PSFCU member information left in their custody.
In response to the PSFCU breach incident:

[1] Palm Springs Federal Credit Union and Sun Community Federal Credit Union (SCFCU) have announced plans to merge with a scheduled effective date of May 1, 2015. SCFCU will remain as the surviving charter.
[2] Palm Springs Federal Credit Union has approximately 1,600 members and $13 million in assets.

- The NCUA Executive Director issued an agency memorandum to all staff regarding the circumstances surrounding the loss of PSFCU member data. The memorandum addressed the agency's required annual security awareness training, "which includes training on the protection of personally identifiable information." The memorandum also indicated that field directors will review certain security policies at their next group meetings and that NCUA plans additional security training in 2015. Furthermore, the Executive Director highlighted that NCUA had conducted more than 28,000 examinations since April 2008 without encountering a notable problem.

- NCUA announced mandatory data breach training in February 2015. NCUA required its staff to complete the training by April 17, 2015.

- NCUA proposed two additional administrative solutions to help minimize the risk of repeating such an incident. Specifically that:

  - Senior management continuously stress the importance of end user situational awareness and consequences of non-compliance with NCUA policies; and

  - NCUA accelerate implementation of the NCUA Privacy Program to increase end user awareness of privacy-related issues.[3]

- NCUA assessed six technical options for securely transferring files.[4]

- NCUA began revising NCUA Instruction 13500.09, Security of External Party's Documentation (March 25, 2008).

OBJECTIVE, SCOPE AND METHODOLOGY

The objective of this audit was to determine whether NCUA has adequate controls in place to protect sensitive, confidential, or personally identifiable electronic credit union information during examinations.

We initiated this audit as a result of the incident involving the breach of Palm Springs Federal Credit Union member information we discussed in the Background section of this report. To accomplish this audit, we conducted fieldwork at NCUA's headquarters in Alexandria, Virginia and with NCUA Regional office management and staff via the NCUA email system. We interviewed management and staff from the Office of the Chief Information Office (OCIO), the Office of Examination and Insurance (E&I), the Office of National Examinations and Supervision (ONES), the Office of Small Credit Union Initiatives (OSCUI), and Regional

[3] NCUA records indicate the agency has been on schedule to implement its Privacy Program by June 30, 2015.
[4] We address NCUA efforts regarding technical solutions in a later section of this report.

offices. We reviewed NCUA regulation, policies, procedures and training associated with protecting sensitive, confidential, or personally identifiable information.[5]

We conducted this review from February 2015 through June 2015 in accordance with generally accepted government auditing standards and included such tests of internal controls as we considered necessary under the circumstances. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

[5] During this audit, we learned NCUA has been in the process of updating NCUA Instruction 13500.09, Security of External Party's Documentation (March 25, 2008) since the PSFCU breach occurred. The OIG did not review the draft Instruction. The intent of this report is to provide NCUA with information and recommendations that would be helpful to NCUA management in the agency's efforts to improve the Instruction.

RESULTS

We determined that NCUA has provided examiners with appropriate tools with which to securely receive electronic information from credit unions during the examination process. However, we also determined:

1. NCUA does not require credit unions to provide sensitive, confidential, and personally identifiable credit union member information to NCUA staff in a protected manner.

2. NCUA needs to improve its policies, procedures and training to help ensure NCUA staff take appropriate measures to protect sensitive, confidential, and personally identifiable electronic credit union member information during examinations; and

3. NCUA needs to improve its guidance to require NCUA staff to use specific tools to transfer sensitive, confidential, and personally identifiable electronic credit union member information during examinations.

Credit Union Electronic Data Protection Standards Needed to Bolster NCUA's Efforts to Protect Member Information

We determined NCUA does not mandate specific credit union security measures. Specifically, NCUA does not require that credit unions: (1) provide sensitive, confidential, and personally identifiable member information in an encrypted or otherwise protected manner; or (2) use available NCUA tools for protecting this information. While NCUA regulation requires that credit unions develop written security programs designed to protect member records, the agency provides only guidelines as to what specific security measures the credit unions must *consider* implementing. As long as credit unions have the option as to whether or not they protect member information they provide to NCUA staff during examinations, there will be continued increased risk of exposing that sensitive information despite NCUA management's efforts to improve the measures the agency takes to protect it.

The Gramm-Leach-Bliley Act (Public Law 106-102 - Section 501(b)) requires the Board of the National Credit Union Administration with respect to any federally-insured credit union to establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards.[6]

To address the Gramm-Leach Bliley Act, NCUA amended 12 CFR Part 748 – "Security Program, Report of Crime and Catastrophic Act and Bank Secrecy Act Compliance" (NCUA Rule). Effective July 1, 2001, this rule requires federally-insured credit unions to develop written security programs that are designed to ensure the security and confidentiality of member records, protect against the anticipated threats or hazards to the security or integrity of such

[6] Public Law 106–102, Title V, § 501, November 12, 1999

records, and protect against unauthorized access to or use of such records that could result in substantial harm or serious inconvenience to a member. NCUA also issued an appendix to the NCUA Rule – Appendix A: "Guidelines for Safeguarding Member Information." This appendix provides guidance standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of member information maintained by or on behalf of federally-insured credit unions that are appropriate to the size and complexity of the credit union and its scope of activities. The appendix indicates that in developing and implementing its member information security program, credit unions *should* [emphasis added] design the program to control identified risks, commensurate with the sensitivity of the information and the complexity and scope of activities. The appendix also indicates that each credit union must *consider* [emphasis added] whether specified security measures are appropriate for the credit union, and if so, adopt them. These measures include encrypting electronic member information while in transit or in storage on networks or systems to which unauthorized individuals may have access.

The NCUA Rule only requires that credit unions *consider* encrypting their member information in transit, which does not afford NCUA staff the option to require that credit unions use - absent credit union tools or other measures - available NCUA data protection tools during examinations. An NCUA management official informed us that it is not uncommon for credit unions to provide data in an unprotected manner. In addition, NCUA recognizes that some credit unions may have policy restricting the use of non-credit union portable devices. Those credit unions that do not take appropriate measures to protect member data on their own or do not allow NCUA staff to use available agency data protection measures will forestall NCUA data protection efforts and ultimately continue to place credit union member information at risk of exposure.

We learned that in response to the Palm Springs Federal Credit Union (PSFCU) data breach, NCUA began reviewing 12 CFR Part 748 to determine whether the agency could mandate the standards currently included as guidelines in Appendix A. NCUA officials recently informed us this review is still in progress.

Recommendations:

We recommend that NCUA management:

1. Require federally-insured credit unions to provide sensitive, confidential, or personally identifiable electronic credit union member information to NCUA/NCUA staff in an encrypted or otherwise secure manner (e.g., file(s) protected with strong password(s)) whether using the credit unions' own secure tools or measures or using available NCUA secure tools or measures.

Management Response:

Management indicated that by July 31, 2015, the Office of Examination & Insurance (E&I) will have updated the initial "Day 1" letter to credit unions to clearly define expectations regarding

the protection of sensitive information during the exam process. Management noted that implementation of the letter depends on completing any bargaining obligation with the National Treasury Employees Union (NTEU).

In addition, management also indicated that they have revised Instruction 13500.09 *Security of Sensitive Information* to more clearly define expectations of staff regarding the protection of sensitive information, noting the instruction will be implemented as soon as any bargaining obligation with NTEU is completed.

Finally, management indicated NCUA is working on a proposed regulation to require all information furnished to NCUA pursuant to Section 741.6 or 748.1 of NCUA's regulations to be encrypted or otherwise provided in a secure manner. NCUA expects that this proposed regulation will be presented at a Board meeting by yearend 2015.

OIG Response:

We concur with management's planned actions.

Improvements Needed to Strengthen NCUA's External Electronic Information Protection Policy

We determined NCUA needs to improve its policies, procedures and training to help ensure NCUA staff take appropriate measures to protect sensitive, confidential, and personally identifiable electronic credit union member information during examinations. Specifically, we determined: (1) NCUA's policies, procedures, and training that address data protection do not fully specify and reinforce requirements or guidelines NCUA staff must adhere to or follow in protecting electronic credit union member information; and (2) NCUA does not adequately stress to staff the importance of protecting credit union member information or the consequences for failing to protect this information. Notwithstanding that NCUA currently does not require credit unions to protect member information as discussed in the previous section, NCUA needs to improve its policies, procedures, and training because they provide only general and limited data protection guidance; the guidance is distributed across several policy or procedure documents; and do not effectively address electronic data protection measures in the context of examiners' job responsibilities. We believe these issues contributed to the NCUA examiners accepting and failing to adequately protect the unsecured device from credit union staff that ultimately resulted in the loss of the PSFCU member information.

NCUA Electronic Data Protection Policies, Procedures, and Training

NCUA Instruction 13500.09, Security of External Party's Documentation (March 25, 2008) (External Data Protection Policy) is meant to serve as an umbrella policy for NCUA's electronic and hardcopy security program. It provides policies and procedures for securing electronic and hardcopy documentation about or acquired from credit unions or any other party external to NCUA (entities). The External Data Protection Policy indicates that NCUA staff must ensure

they properly secure confidential and sensitive information of other entities to prevent disclosing that information to unauthorized parties. The External Data Protection Policy specifies that:

- Any electronic device or physical storage device which contains an organization's sensitive or confidential information must be properly secured and controlled at all times;

- When requesting an entity to forward, send, or deliver electronic documents containing confidential or sensitive information, NCUA staff will *recommend* [emphasis added] the documents be provided in a secure manner such as encrypted email or file;

- Electronic documents - in transit and in storage - containing sensitive or confidential information must be maintained in an encrypted manner.

NCUA's Rules of Behavior (NCUA Rules document) addresses privacy and security obligations and specific computer security controls that must be followed when collecting, maintaining, using, or distributing agency information in electronic or physical form. The NCUA Rules document advises NCUA device users that they are responsible for ensuring that their activities do not circumvent NCUA information security controls or violate any rules described within the NCUA Rules document. The NCUA Rules document also indicates the following:

- When using electronic share and loan data during an AIRES[7] examination, staff must treat this data as confidential;

- Staff must follow the information safeguards required by management such as keeping designated information in a secured office, locked file drawer or cabinet, or in a password protected electronic file;

- Staff must protect electronic and physical records - which may contain PII - from unauthorized access and use;

- NCUA employees are responsible for protecting the confidentiality of PII. NCUA will hold employees, supervisors, managers, contractors and state supervisors accountable for safeguarding PII;

- Managers are responsible for providing practical guidance to their employees in a job-related context, specifically identifying PII and its authorized collection, access, use, disclosure, storage, and destruction; and

[7] NCUA and state examiners use the Automated Integrated Regulatory Examination System to review and validate financial data related to the operations of federally insured credit unions and some state-chartered, non-federally insured credit unions.

- Employees are responsible for adhering to administrative, technical, and physical safeguards to ensure only authorized persons have access to records and information is used and disclosed only as authorized.

NCUA's Information Security Policy (July 8, 2014) (NCUA Handbook) defines the policies necessary for NCUA employees to meet the fundamental security and privacy objectives of confidentiality, integrity, and availability of NCUA information and information resources. The NCUA Handbook applies to digital and non-digital data that NCUA owns, sends, receives or processes, and:

- Indicates "All NCUA information in printed form or on digital media shall be protected within and outside of NCUA facilities.";
- Indicates that violations of the policies may result in the loss or limitation of access to NCUA information systems and information;
- Indicates that anyone who violates NCUA policies may face administrative action ranging from counseling, to removal from NCUA, as well as criminal penalties or financial liability, depending on the severity of misuse; and
- Indicates NCUA employees (and contractors) are subject to penalties established by the Privacy Act of 1974.[8]

NCUA Instruction 01200.15, Rules and Consequences for Safeguarding Personally Identifiable Information (October 5, 2007) establishes policy and guidance regarding the consequences and corrective actions for employees, supervisors, and managers who fail to safeguard PII. The Instruction indicates:

- It is NCUA's policy to safeguard PII the agency possesses in paper or electronic format and to prevent the breach of such information;
- Managers and supervisors are responsible for instructing, training, and supervising employees on safeguarding PII; and
- The applicable consequences for failing to safeguard PII include a letter of reprimand, suspension or removal.

NCUA requires and provides security awareness training (security training) to new employees and to all NCUA staff annually thereafter. Regarding private data, the security training: (1) defines PII; (2) identifies "types" of private data (i.e., "PII, medical records and personal financial information are the most common types…"); and (3) indicates that digital private data

[8] Certain penalties apply to the misuse or unauthorized disclosure of PII. The Act (5 U.S.C. 552a (g)) provides for civil remedies for injured parties, including actual damages, attorney fees, and litigation costs.

should always be protected (via password and encryption). The security training also indicates that working in public places exposes users to additional risks, and users should never leave mobile data devices in view.

NCUA requires and provides annual Privacy training to NCUA staff. The Privacy training provides examples of how data breaches occur and includes the following guidance for protecting private data:

- Nonpublic information, which could be confidential (e.g., personal financial records), must be handled with great care;
- PII is a type of private data, and "…personnel records and customer account records are private and must be kept confidential.";
- "[G]eneral rules for handling" private data, (e.g., maintain the confidentiality of customer's private data, use physical and technical safeguards to ensure the confidentiality and integrity of private data, etc.);
- Data storage guidance, i.e., lock up documents; protect files with a password; and encrypt data on mobile devices; and
- Guidance for transmitting privacy data, (i.e., "Avoid sending private data through non-secure channels….").

OIG Assessment of NCUA's Electronic Data Protection Policies, Procedures, and Training

We assessed NCUA's policies, procedures, and training for adequacy of their data protection content as follows:

- NCUA Instruction 13500.09 (External Data Protection Policy) is outdated; includes limited directive policy and procedures to NCUA staff for protecting sensitive, confidential, or personally identifiable electronic credit union member information in the context of examiners' job responsibilities; and does not adequately address the consequences for failing to protect this information. Specifically:
    - The External Data Protection Policy does not include requirements or guidance for NCUA staff to: (1) use any particular procedures to digitally protect (e.g., encrypt, password protect, etc.) electronic credit union member information; or (2) take specific alternate measures to ensure the secure receipt of credit union member information in the event the staff is unable to use or ensure that credit union staff use encryption or other secure measures to protect credit union member information. As indicated above, the External Data Protection Policy generically indicates that: (1) an electronic device containing sensitive or confidential information must be protected;

and (2) when requesting an entity to forward, send, or deliver documents containing confidential or sensitive information, NCUA staff will *recommend* [emphasis added] the entity *send* [emphasis added] documents in a secure manner.

- Although NCUA prominently addresses consequences for violating NCUA data protection policies in the NCUA Handbook, the External Data Protection Policy provides only a footnote reference to a list of other NCUA Instructions including NCUA Instruction 01200.15, Rules and Consequences for Safeguarding Personally Identifiable Information.

- The NCUA Handbook and the NCUA Rules document provide NCUA staff with only general guidance that they must take measures to protect sensitive and confidential information, e.g., treat AIRES exam data as confidential; follow required information safeguards such as password protected files; protect NCUA information on digital media, etc.

- Similar to NCUA's External Data Protection Policy, NCUA training provides general guidance in regards to protecting electronic private data and does not provide specific required measures or guidance to protect electronic data. The training also does not adequately stress the importance of protecting credit union member information or reinforce the consequences for failing to protect this information. Specifically:

  - NCUA indicates that "Training ensures that all employees are not only aware of information security issues, but also know *how to address issues within the context of their job responsibilities* [emphasis added]." However, as indicated above, the annual security awareness training provides only general information regarding the privacy of data and very brief and general guidance that private data should be protected. In addition, we noted that while the security training indicates that NCUA employees and contractors are responsible for understanding and following the policy standards set forth in the NCUA Rules document and the NCUA Handbook, the training makes no such reference to NCUA's External Data Protection Policy. Furthermore, the security training does not effectively stress the importance of protecting credit union member information or reinforce NCUA policy regarding the consequences for failing to protect this information.

  - As indicated above, the Privacy training addresses general rules for handling, storing, and transmitting private data. However, the Privacy training does not: (1) sufficiently-stress the importance of protecting credit union member information; (2) address or reinforce NCUA policy regarding the consequences and corrective actions for NCUA employees, supervisors and managers who fail to safeguard PII or who violate NCUA policy for protecting sensitive information; or (3) address potential consequences NCUA and credit unions face if NCUA staff fail to protect sensitive credit union member information (e.g., damage to NCUA's and/or a credit

unions' reputation/image, loss of credit union members; and the financial impact associated with data breach notification, investigating the data breach, litigation, etc.).

The NCUA staff members involved in the PSFCU incident indicated that in their experience with examinations, smaller credit unions (e.g., PSFCU[9]) are more likely to provide electronic credit union data unprotected on a digital device while larger credit unions use secure methods.[10] An NCUA management official also indicated it is not uncommon for credit unions to provide data in an unsecure manner. Another NCUA official informed the OIG that – as discussed above - NCUA does not require credit unions to use NCUA data protection measures or to even provide credit union member information in a secure manner using other data protection measures. As previously indicated, we believe that the general, limited, and distributed nature of NCUA's data protection policies and procedures and the lack of adequate reinforcement regarding significant consequences associated with losing or exposing credit union member information may have contributed to allowing and accepting insecure procedures that ultimately resulted in the loss of the sensitive PSFCU member information. In the PSFCU incident, the examiners accepted the unprotected flash drive from PSFCU staff rather than use available NCUA secure tools (as discussed in the next section of the report) or alternate secure measures.

Although NCUA cannot currently compel credit unions to take any particular measures/steps to provide sensitive credit union member information in a secure manner during examinations, we believe that by requiring specific data protection measures or alternate practical steps to protect electronic credit union member information during examinations; periodically reinforcing these specific measures/steps; and stressing and periodically reinforcing to NCUA staff the consequences for violating NCUA electronic data protection policies, NCUA could help mitigate the potential exposure of sensitive, confidential, or personally identifiable credit union member information in the future.

Recommendations:

We recommend that NCUA management:

2. Complete the revision of NCUA Instruction 13500.09 to consolidate, include or reference: (1) specific policy, procedure or alternate practical guidance – depending on the examination scenario – agency staff must adhere to or follow to help ensure the protection of sensitive, confidential, and personally identifiable electronic credit union member information; and (2) the consequences NCUA staff face for failing to follow NCUA requirements, procedures, or guidance for protecting credit union member information.

[9] As previously noted, Palm Springs Federal Credit Union has approximately 1,600 members and $13 million in assets.

[10] An NCUA manager informed the OIG that there is a concern regarding the financial burden that would be placed on smaller credit unions if they were required to purchase encrypted devices.

Management Response:

Management indicated that NCUA revised Instruction 13500.09 and will implement it after completing any bargaining obligation with NTEU.

OIG Response:

We concur with management's planned action.

3. Enhance NCUA annual security awareness training or provide additional supplementary periodic training that reinforces credit union data protection requirements established in NCUA Instruction 13500.09 and provides NCUA staff with "practical guidance" for addressing "issues within the context of their job responsibilities" as they handle sensitive, confidential, and personally identifiable electronic credit union member information throughout the examination process.

Management Response:

Management indicated that the Office of the Chief Information Officer (OCIO) will update the annual security training to incorporate all recommended enhancements. This updated training will be utilized in the 2015 annual security training, due to be performed by yearend 2015.

OIG Response:

We concur with management's planned action.

4. Enhance annual Privacy training to stress the importance of protecting sensitive credit union member information; address and reinforce to NCUA staff the consequences for violating/failing to follow NCUA policy, requirements and procedures for protecting sensitive credit union member information; and address potential consequences NCUA and credit unions also face if staff fail to protect sensitive credit union member information.

Management Response:

Management indicated that the Senior Agency Official for Privacy (SOAP) will update the annual Privacy training to incorporate all the recommended content changes. This update training will be utilized in the 2015 annual Privacy training, due to be performed by yearend 2015.

OIG Response:

We concur with management's planned action.

Improvements Needed to Require Tools for Securely Exchanging Electronic Credit Union Information

We determined NCUA has provided agency staff with appropriate tools for securely receiving electronic information from credit unions during the examination process. Specifically, NCUA has provided NCUA employees with an encrypted flash drive and an email encryption solution. However, NCUA has not provided sufficient guidance to staff regarding under what circumstances it is appropriate or required to use these available tools in protecting sensitive, confidential, or personally identifiable electronic credit union member information during the examination process nor does the agency effectively remind staff that these tools are available. NCUA's External Data Protection policy does not address the use of these tools. In addition, while other NCUA policies that pertain to electronic data protection do address the availability of these tools, none of these documents require or guide when NCUA staff should use them. Furthermore, NCUA annual security training does not address/reinforce the use of these tools. We believe that if NCUA requires and provides guidance to staff to use the appropriate secure tool (or alternate measures) to protect electronic credit union member information during examinations, NCUA could help mitigate the chance that NCUA staff will settle on insecure measures for receiving sensitive, confidential, or personally identifiable electronic credit union member information during the examination process.

NCUA Electronic Data Protection Policies and Procedures

NCUA Instruction 13500.09, Security of External Party's Documentation (March 25, 2008) (External Data Protection Policy) is meant to serve as an umbrella policy for NCUA's electronic and hardcopy security program. It provides policies and procedures for securing electronic and hardcopy documentation about or acquired from credit unions or any other party external to NCUA.

NCUA Instruction 13302.1 (REV), Electronic Mail, Communications, and Filing/Storage of Electronic Documents (April 1, 1996) (NCUA eMail Policy) establishes standardized policies and procedures on the usage of electronic mail and communications by NCUA staff.

The NCUA Communications Manual – Procedures and Requirements for NCUA Communications Products (Revised December 2014) (NCUA Communications Manual) provides NCUA staff with an understanding of how to handle agency correspondence. It includes a chapter specific to Email and Electronic Communications Procedures, which addresses secure email procedures.

NCUA's Hi-Tech Handbook includes care and maintenance procedures for NCUA assigned hardware; documentation for third party purchased software; and documentation on peripherals issued to NCUA staff. The Hi-Tech Handbook includes specific procedures for using NCUA's secure email system and its secure flash drives.

Encrypted Email Solution

NCUA has had a [redacted] email encryption service [redacted] in place since at least 2008. The [redacted] is a secure email process that allows NCUA staff to send (and receive) encrypted emails. The [redacted] Crypto Module, a component of the [redacted], provides email encryption using a Federal Information Processing Standards[12] (FIPS) 140-2[13] validated cryptographic module, which includes an approved Advanced Encryption Standard (AES[14]) algorithm. NCUA employees can encrypt agency email they send to any recipient outside of the NCUA email system [redacted]. If the recipient does not have a [redacted], they must register to send and receive secure messages by creating a password for access to the NCUA secure message center to retrieve the secure email. The recipient facilitates this access by clicking on the link within the [redacted] they receive. Once the recipient sets up their access, they will have continued access to encrypted emails provided through the [redacted]. Recipients who have a [redacted] would receive the encrypted email directly. The recipient's reply to the secure email encrypts the response.

Encrypted Flash Drives

NCUA has provided NCUA employees with encrypted flash drives [redacted] - since approximately 2008. The flash drive is standard issue equipment for NCUA examiners. The [redacted] drive is FIPS 197 validated.[15] The device provides 256-bit AES hardware-based encryption, requires the use of a complex password to prevent unauthorized access to the data, and locks down and reformats the device [redacted].

OIG Assessment of NCUA Data Protection Policies, Procedures, and Training

We assessed NCUA's policies, procedures, and training for content related to tools for securely transferring electronic information as follows:

[redacted]

[12] Federal Information Processing Standards are standards and guidelines that NIST develops for Federal computer systems. NIST develops FIPS when there are compelling Federal government requirements such as for security and interoperability and there are no acceptable industry standards or solutions.

[13] The name of the FIPS 140-2 standard is *Security Requirements for Cryptographic Modules*. Products validated as conforming to FIPS 140-2 are accepted by the Federal agencies of the United States and Canada for the protection of sensitive information (United States) or Designated Information (Canada).

[14] The *NIST Advanced Encryption Standard* specifies a FIPS-approved algorithm for use in protecting electronic data.

[15] FIPS 197 is the *NIST Advanced Encryption Standard*.

- NCUA Instruction 13500.09 (External Data Protection Policy) is outdated and does not include guidance as to which NCUA tools are appropriate or required under various circumstances to protect credit union member information. Specifically:

  - NCUA has not updated the March 2008 External Data Protection Policy to direct and guide the staff to use tools (i.e., encrypted email and secure flash drives) the agency has made available since at least 2008 for securely transferring electronic information and under what circumstances the tools are required or appropriate. For example, the External Data Protection Policy generically indicates that there are numerous programs or applications that can be used to encrypt email. It also states that OCIO is working to secure an encryption program [redacted] that entities *can* [emphasis added] use to send encrypted items via email.

  - The 2008 External Data Protection Policy references an April 1, 1996 NCUA Instruction 13302.1 (REV) (NCUA eMail Policy), which in terms of protecting electronic data merely advises that it is best to use caution and discretion when sending sensitive information via email. However, the NCUA Communications Manual has delineated the procedures for sending and receiving secure emails via the agency's email encryption service since January 2013.
- Although NCUA indicates that training ensures that employees know how to address information security issues within the context of their job responsibilities, the annual security training does not address/reinforce the availability, use, or applicability of NCUA's secure tools for protecting electronic credit union member information during examinations.

We learned that in response to the PSFCU data breach, the OCIO proposed and assessed the following six technical options to address the issue of securely transferring files:

- Require all credit unions to encrypt all data before submitting the data to NCUA examiners;

- Lock down all NCUA laptops and devices to require NCUA examiners to use only encrypted USB devices (ideally NCUA-approved devices) to obtain data from credit unions;

- Configure NCUA laptops to automatically encrypt USB devices that are unencrypted;

- Implement a centrally managed encryption solution (e.g. IronKey, Symantec, Checkpoint) to remotely manage encrypted USB devices;

- Implement a secure file transfer solution;[16] and

- If all other technical options are not viable, provide NCUA examiners with technical training on how to encrypt credit union data upon receipt.

The OCIO informed the OIG that NCUA has opted to pursue a secure file transfer solution for all NCUA users and credit unions. NCUA indicated the goal is to replace USB drives as the primary means of file transfer between credit unions and examiners. NCUA's primary requirements for its secure file transfer platform are as follows:

- Send and receive large non-sensitive files to and from large external entities;

- Send and receive sensitive files to and from external entities;

- Allow credit unions to send sensitive files to NCUA in a controlled, secure manner; and

- Easy to use, user-driven application.

OCIO staff indicated NCUA conferred with other federal agencies (e.g., the U.S. Securities and Exchange Commission, the Federal Deposit Insurance Corporation, the Federal Housing Finance Agency, the Federal Reserve Board, and the U.S. Commodity Futures Trading Commission) regarding secure file transfer solutions. OCIO staff added that NCUA considered cloud-based systems[17] and on premise systems. OCIO staff indicated that none of these agencies use the cloud for sensitive information. During the course of this audit, OCIO narrowed its potential vendors from eight to two. NCUA is recommending pilot testing the products from those two vendors – [redacted].[18]

A key component of the [redacted] Cryptographic Module, which is FIPS 140-2 validated. It enables organizations to securely share and transfer files. [redacted] obtains cryptographic services from [redacted] Cryptographic Module, which is also FIPS 140-2 validated. The services include symmetric/asymmetric encryption/decryption.

As previously mentioned, we learned that when considering possible technical solutions for securely transferring credit union information, NCUA recognized that credit unions may have policy restricting the use of non-credit union portable devices. If credit unions do not have their own secure tools or alternate secure measures, we believe there is continued risk that credit union

[16] We learned that prior to the incident, NCUA had been researching a secure file transfer platform based on specific requests from two of the agency's directorates.
[17] "Cloud-based" refers to applications, services or resources made available to users on demand via the Internet from a service provider's servers. Companies typically use cloud-based computing as a way to increase capacity, enhance functionality, or add additional services on demand without having to commit to potentially expensive infrastructure costs or increase/train existing in-house support staff.
[18] NCUA's milestone indicates implementing a solution by the end of the third Quarter of 2015.

or NCUA staff may be tempted to settle on an insecure method to transfer member information. By requiring and providing guidance to NCUA staff to use the appropriate secure tool to protect the transfer of electronic credit union member information under the appropriate circumstances during examinations, we believe NCUA could help mitigate the chance that NCUA staff will settle on insecure measures for exchanging sensitive, confidential, or personally identifiable electronic credit union member information. We also believe that by adopting an additional secure tool that is readily accessible by both NCUA and credit union staff during examinations, NCUA could further mitigate the chance of exposing sensitive, confidential, or personally identifiable electronic credit union member information.

Recommendations

We recommend NCUA management:

5. Continue to pursue and implement the secure file transfer solution NCUA is assessing to transfer sensitive, confidential, or personally identifiable electronic credit union member information.

Management Response:

Management indicated that OCIO will complete the implementation of the secure file transfer solution by Yearend 2015.

OIG Response:

We concur with management's planned action.

6. Complete the revision of NCUA Instruction 13500.09 to require and provide guidance on secure tools or alternate procedures NCUA staff must use under various circumstances to transfer sensitive, confidential, or personally identifiable electronic credit union member information during examinations.

Management Response:

Management indicated that NCUA revised Instruction 13500.09 and will implement it after completing any bargaining obligation with NTEU.

OIG Response:

We concur with management's planned action.

7. Enhance NCUA annual security awareness training to reinforce to NCUA staff the availability, use, and applicability of secure NCUA tools to transfer sensitive, confidential, or personally identifiable electronic credit union member information.

Management Response:

Management indicated that OCIO will update the annual security training to address all recommended enhancements. This updated training will be utilized in the 2015 annual security training, due to be performed by yearend 2015.

OIG Response:

We concur with management's planned action.

Appendix A: NCUA Management Response

OCIO
SSIC 13500

SENT BY E-MAIL

TO: Inspector General Jim Hagen

FROM: Executive Director Mark Treichel Mark Treichel

SUBJ: Audit of the National Credit Union Administration's Measures to Protect Electronic Credit Union Member Information During the Examination Process

DATE: June 8, 2015

This memorandum responds to your request for comment on the report entitled, *Audit of the National Credit Union Administration's Measures to Protect Electronic Credit Union Member Information During the Examination Process*. Thank you for the opportunity to review and comment on the report's findings and recommendations. We concur with the recommendations and the following is our plan to address them.

OIG Report Recommendation #1

Require federally-insured credit unions to provide sensitive, confidential, or personally identifiable electronic credit union member information to NCUA/NCUA staff in an encrypted or otherwise secure manner (e.g., file(s) protected with strong password(s)) whether using the credit unions' own secure tools or measures or using available NCUA secure tools or measures.

Response: By July 31, 2015, the Office of Examination & Insurance (E&I) will update the initial "Day 1" letter to credit unions to clearly define expectations regarding the protection of sensitive information during the exam process. Implementation of the letter depends on completing any bargaining obligation with the National Treasury Employees Union (NTEU).

NCUA revised Instruction 13500.09 *Security of Sensitive Information* to more clearly define expectations of staff regarding the protection of sensitive information. The instruction will be implemented as soon as any bargaining obligation with NTEU is completed.

NCUA is working on a proposed regulation to require all information furnished to NCUA pursuant to Section 741.6 or 748.1 of NCUA's regulations to be encrypted or otherwise provided in a secure manner. NCUA expects that this proposed regulation will be presented at a Board meeting by yearend 2015.

OIG Report Recommendation #2

Complete the revision of NCUA Instruction 13500.09 to consolidate, include or reference: (1) specific policy, procedure or alternate practical guidance – depending on the examination scenario – agency staff must adhere to or follow to help ensure the protection of sensitive, confidential, and personally identifiable electronic credit union member information; and (2) the

consequences NCUA staff face for failing to follow NCUA requirements, procedures, or guidance for protecting credit union member information.

Response: NCUA revised Instruction 13500.09 and will implement it after completing any bargaining obligation with NTEU.

OIG Report Recommendation #3

Enhance NCUA annual security awareness training or provide additional supplementary periodic training that reinforces credit union data protection requirements established in NCUA Instruction 13500.09 and provides NCUA staff with "practical guidance" for addressing "issues within the context of their job responsibilities" as they handle sensitive, confidential, and personally identifiable electronic credit union member information throughout the examination process.

Response: The Office of the Chief Information Officer (OCIO) will update the annual security training to incorporate all recommended enhancements. This updated training will be utilized in the 2015 annual security training, due to be performed by yearend 2015.

OIG Report Recommendation #4

Enhance annual Privacy training to stress the importance of protecting sensitive credit union member information; address and reinforce to NCUA staff the consequences for violating/failing to follow NCUA policy, requirements and procedures for protecting sensitive credit union member information; and address potential consequences NCUA and credit unions also face if staff fail to protect sensitive credit union member information.

Response: The Senior Agency Official for Privacy (SAOP) will update the annual Privacy training to incorporate the recommended content changes. This updated training will be utilized in the 2015 annual Privacy training, due to be performed by yearend 2015.

OIG Report Recommendation #5

Continue to pursue and implement the secure file transfer solution NCUA is assessing to transfer sensitive, confidential, or personally identifiable electronic credit union member information.

Response: OCIO will complete the implementation of the secure file transfer solution by Yearend 2015

OIG Report Recommendation #6

Complete the revision of NCUA Instruction 13500.09 to require and provide guidance on secure tools or alternate procedures NCUA staff must use under various circumstances to transfer sensitive, confidential, or personally identifiable electronic credit union member information during examinations.

Response: NCUA revised Instruction 13500.09 and will implement after completing any bargaining obligation with NTEU.

OIG Report Recommendation #7

Enhance NCUA annual security awareness training to reinforce to NCUA staff the availability, use, and applicability of secure NCUA tools to transfer sensitive, confidential, or personally identifiable electronic credit union member information.

Response: OCIO will update the annual security training to address all recommended enhancements. This updated training will be utilized in the 2015 annual security training, due to be performed by yearend 2015.

If you have any questions, please do not hesitate to contact my office.