August 10, 2016

SENT BY EMAIL

The Honorable Jason Chaffetz
Chairman
Committee on Oversight and Government Reform
U.S. House of Representatives
2157 Rayburn House Office Building
Washington, DC 20515

The Honorable Ron Johnson
Chairman
Committee on Homeland Security and Governmental Affairs
United States Senate
340 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Elijah E. Cummings
Ranking Member
Committee on Oversight and Government Reform
U.S. House of Representatives
2471 Rayburn House Office Building
Washington, DC 20515

The Honorable Thomas R. Carper
Ranking Member,
Committee on Homeland Security and Governmental Affairs
United State Senate
340 Dirksen Senate Office Building
Washington DC 20510

Dear Chairman Chaffetz, Chairman Johnson, Representative Cummings, and Senator Carper:

This letter represents the National Credit Union Administration (NCUA) Office of Inspector General's (OIG) response to the reporting requirements set forth at § 406 of the "Cybersecurity Act of 2015", Pub. L. No. 114-113, (the Act). Section 406(b)(1) requires Inspectors General of covered agencies to submit a report to include specific information regarding their respective agency's Federal computer systems.

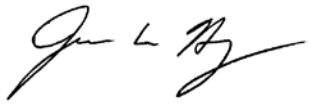
In accordance with § 406(b)(2) of the Act, this response addresses: (1) NCUA-owned covered systems[1] and (2) covered systems a third-party (contractor or other Federal agency) owns, operates, and/or manages on NCUA's behalf that processes, stores, or transmits NCUA information. We have included listings of these systems in Attachment A (NCUA-owned covered systems) and Attachment B (Third-party covered systems).

We relied on our 2015 "Federal Information Systems Modernization Act" (FISMA) audit work to address our responses where applicable. We also obtained, as necessary, additional information from NCUA officials to complete our responses. Because of the sensitive nature of the technical information contained in our response, we are including our responses in Attachment C.

[1] The Act at § 406(a)(1) defines a covered system as "a national security system as defined in section 11103 of title 40, United States Code, or a Federal computer system that provides access to personally identifiable information."

Should you wish additional information on our responses, please do not hesitate to contact me at (703) 518-6351 or Marvin Stith, Senior IT Auditor, at (703) 518-6359.

Sincerely,



James W. Hagen
Inspector General

Attachments

cc: The Honorable Richard Shelby, Chairman, Senate Committee on Banking, Housing, and Urban Affairs
The Honorable Sherrod Brown, Ranking Member, Senate Committee on Banking, Housing, and Urban Affairs
The Honorable Jeb Hensarling, Chairman, House Financial Services Committee
The Honorable Maxine Waters, Ranking Member, House Committee on Financial Services

Attachment A: NCUA-Owned Covered Systems

NCUA-Owned Systems	
System Name	**Acronym**
General Support System	GSS
The GSS provides infrastructure and platform centric access controls to NCUA's network. It provides the common security controls for all significant NCUA business systems, e.g. networking, storage, servers, virtualization, operating systems, middleware, and runtime components while the system owners typically provide system specific controls for data and applications.	
The following NCUA systems leverage the GSS infrastructure access controls and implement other application-level system specific controls.	
• Asset Liquidation Management System	ALMS
Provides the computing platform for the accounting of credit unions involved in the process of liquidation and all significant business applications of NCUA's Asset Management and Assistance Center.	
• Automated Integrated Regulatory Examination System	AIRES
Enables examiners to review and validate the financial status of credit unions.	
• Call Report System	CU Online
The primary means to collect, validate, store, and report quarterly financial and operational data for all federally insured credit unions (FICUs) and some state-chartered, non-federally insured credit unions (NFICUs).	
• Credit Union Service Organization Registry	CUSO Registry
The online system through which a credit union service organization (CUSO) reports information about the CUSO directly to NCUA.	

Attachment B: Third-Party[1] Covered Systems

Third-Party Systems (Contractor/Federal)		
System Name	**Acronym**	**Service Provider**
BudgetPak™		Xlerant
NCUA uses BudgetPak for its budget formulation function.		
Comprehensive Human Resources Integrated System	CHRIS	GSA
Agencies use CHRIS to document employee employment history. Employees can also use CHRIS to access their personnel records from their desktops.		
Concur Travel and Expense		Concur Technologies, Inc.
The system NCUA uses for travel and expense management.		
CyberGrants		CyberGrants, Inc.
Assists NCUA in managing funding requests for its Grant and Loan Program.		
Delphi		DoT
Shared service accounting system NCUA uses for managing its general ledger, accounts receivable, accounts payable and fixed assets, and for complying with federal reporting requirements.		
Electronic Official Personnel Folder	eOPF	OPM
An electronic version of employees' paper Official Personnel Folder and a system for accessing the electronic folder online.		
Electronic Performance Management System	ePerformance	Northrop Grumman Corp.
Enables employees to complete all phases of NCUA's performance management program via a web-based interface.		

[1] External systems another agency, contractor, or other organization uses and operates on behalf of NCUA, and that processes, stores, or transmits NCUA information.

Employee Express		OPM
Federal employees use Employee Express to make electronic personnel and payroll transactions.		
Employees' Compensation Operations and Management Portal	ECOMP	DoL OWCP
Provides Federal agencies with a comprehensive electronic system for recording workplace injuries and illnesses, and processing claims under the Federal Employee's Compensation Act.		
Financial Disclosure Management System	FDM	DoD
Enables authorized users to electronically file and maintain required financial disclosure reports.		
FOIAXpress		AINS, Inc.
Enables NCUA's Office of General Counsel to manage the entire lifecycle of an initial FOIA request to the final delivery of information to the requestor. The system is also able to produce the Department of Justice Annual FOIA Report.		
Integrity		OGE
Financial disclosure system created by the U.S. Office of Government Ethics (OGE) to house the contents of all public financial disclosure filers in an electronic format.		
Micropact i-complaints® EEO/RA Case Management		MicroPact
NCUA's EEO and Reasonable Accommodation case management solution that automates the EEO process and generates the Form 462 and No FEAR annual report.		
NCUA Learn Center		Oracle America
NCUA uses this system to conduct, store and track employee training.		
Pay.gov		Department of Treasury Bureau of Fiscal Service
Service used to make secure electronic payments to federal government agencies. The system processes loan payments to NCUA's Asset Management and Assistance Center's Treasury account.		

Personnel and Security System	PASS	MicroPact
PASS is a commercial off the shelf application for recording critical screening decisions and adjudicatory functions, and providing case management, and for tracking background investigations conducted on NCUA employees and contractors.		
Salesforce		Salesforce
NCUA uses Salesforce to support the submission and tracking of consumer inquiries and formal complaints against credit unions via the agency's Consumer Assistance Center.		
Send Word Now – SWN Emergency Notification System		Send Word Now
Alerting service provides two-way, on-demand emergency and routine messaging to a designated group of recipients across a variety of platforms.		
USAccess		Hewlett Packard Enterprise (GSA[2])
The GSA-managed Identity, Credentials, and Access Management system NCUA uses for the creation, enrollment, issuance, and maintenance of PIV Credentials.		

[2] The GSA HSPD-12 Managed Service Office (MSO) is the executive agent responsible for managing government-wide acquisition of information technology to implement HSPD-12 services. The GSA HSPD-12 MSO established the USAccess program as an efficient way for Federal agencies to issue common HSPD-12 approved credentials to their employees and contractors.

Attachment C: Responses to Information Requested Under the "Cybersecurity Act of 2015", Pub. L. No. 114-113

A. <u>A description of the logical access policies and practices used by the covered agency to access a covered system, including whether appropriate standards were followed.</u>

- Table C1 below includes the description of the logical access policies and practices and select access control security configuration parameters for NCUA's General Support System (GSS).

- Table C2 below includes NCUA's other four (4) "covered systems." These systems leverage the GSS infrastructure access controls. The table includes other application-level controls specific to these systems.

  Federal Standards:

  - NIST 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013) provides guidelines for selecting and specifying [access] security controls designed to facilitate compliance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

  - OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007) requires remote access only with two-factor authentication.

  - Homeland Security Presidential Directive-12: *Policy for a Common Identification Standard for Federal Employees and Contractors* (August 27, 2004) requires the use of identification by Federal employees and contractors that meets the HSPD-12 Standard in gaining logical access to Federally controlled information systems.

  - OMB M-11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors* (February 3, 2011) requires each agency to develop and issue a policy by March 31, 2011, through which the agency will require the use of the PIV credentials as the common means of authentication for access to that agency's facilities, networks, and information systems.

- During our prior FISMA audit work, we determined:

  - Except as indicated directly below, NCUA follows federal access control requirements as specified in NIST 800-53, Revision 4, Homeland Security

Presidential Directive-12 (HSPD-12), and specified Office of Management and Budget (OMB) memoranda as applicable.

- [redacted]
  - [redacted]

Table C1: General Support System (GSS) Access Control Policies and Procedures

Authentication[4]	
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]

NIST 800-53, Revision 4 Access Controls[5]
Account Management
NCUA tracks access control requests associated with granting, changing, and disabling access [redacted]
Access Enforcement
The NCUA network is configured to enforce information flow within system components and applications [redacted]
Separation of Duties
NCUA implements separation of duties [redacted] NCUA achieves separation of duties as follows:
• Managers and authorized access approvers initiate access requests.
• Security personnel responsible for administering access control do not perform audit functions.
• Office of the Chief Information Officer (OCIO) maintains a limited group of administrators [redacted]
• OCIO maintains separate IT Help Desk and IT Operations teams.
• OCIO ensures that information system [redacted] are divided among separate individuals or groups.
• An independent, external vendor conducts [redacted]
• An independent entity (and not the code developer) conducts quality assurance and code reviews [redacted]
Least Privilege
Access rights to the NCUA network and systems are restricted [redacted] At a minimum:

[5] The System Security Plan (March 16, 2015) for NCUA's General Support System identifies these access controls as implemented within NCUA's Information Technology environment. We assess these controls at least annually during our FISMA audits. In preparation for this response, we queried NCUA for updated information as applicable.

- NCUA must explicitly authorize access to its security functions (deployed in hardware, software, and firmware) and security-relevant information:
  - NCUA grants all employees and contractors using NCUA systems access based on approvals by their managers.
  - NCUA grants user accounts access to specific applications and functions necessary for the performance of official duties.
  - NCUA enforces role-based access [redacted]
- NCUA disables any file system access that is not explicitly required for system, application, and administrator functionality.
- NCUA provides minimal system and physical access to [redacted] who must agree to and support NCUA's security requirements.
- NCUA restricts the use of database management utilities [redacted]
- NCUA prevents users from accessing database data files [redacted]
- NCUA requires that users of information system accounts, or roles, with access to security functions or security-relevant information [redacted]
- NCUA audits any [redacted]

Unsuccessful Logon Attempts:

NCUA enforces three account lockout policies for unsuccessful login attempts:

- [redacted]
  - [redacted]
  - [redacted]

- Laptops:
  - NCUA [redacted] encrypts hard drives with a cryptographic key.
  - A user [redacted] locks access to the laptop.
- iPhones:
  - NCUA-issued iPhones are encrypted.
  - A user [redacted] locks access to the iPhone.

System Use Notification

NCUA has implemented a system use notification banner that applies to all NCUA information systems. With the exception of the public website, users are notified with a warning banner that they are about to access a government-owned information system. [redacted]

Session Lock

The NCUA network is configured to lock workstation sessions [redacted] Users must re-authenticate to the system to unlock their session.

iPhones are configured to automatically lock the screen [redacted]

Session Termination

The VPN that allows remote users to access the system will be configured to disable [redacted]

Remote Access

NCUA allows remote access to [redacted] NCUA grants remote access to the following NCUA user groups:

- [redacted]
- [redacted]

[redacted]

privileged accounts after their regular accounts are authenticated.

[redacted]

Wireless Access

[redacted]

[redacted]

Use of External Information Systems

[redacted]

Information Sharing

NCUA controls information sharing among NCUA users [redacted]

NCUA's [redacted] automatically encrypts outbound emails [redacted]

[redacted]

[redacted]

Security Configuration Parameters		
Parameter	**Setting**	**Meets US Government Configuration Baseline Standards[7]**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[7] The United States Government Configuration Baseline (USGCB) initiative establishes security configuration baseline settings for Information Technology products widely deployed across the federal agencies. The USGCB evolved from the Federal Desktop Core Configuration (FDCC) mandate.

Table C2: System-Specific Access Control Policies and Procedures applicable to NCUA's four (4) other "Covered Systems" that leverage the GSS infrastructure access controls.

Automated Integrated Regulatory Examination System (AIRES)
[redacted]
Account Management
Leverages the GSS infrastructure access control and AIRES application-level (system specific) controls.
NCUA provides all employees with access to the system when employees enter duty with NCUA.
For [redacted] who must approve the requests.
Separation of Duties
The system maintains separation of duties [redacted]
Asset Liquidation Management System (ALMS)
[redacted]
Account Management
Leverages the GSS infrastructure access control and ALMS application-level (system specific) controls.
[redacted]
[redacted]
Separation of Duties
The system maintains separation of duties [redacted]

Least Privilege
The access request form determines whether a user can add, edit, or read information.
Call Report System (CU Online)
[redacted]
[redacted]
Leverages the GSS infrastructure access control and CU Online application-level (system specific) controls.
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
Separation of Duties
The GSS and the system control this function.
[redacted]
[redacted] the system controls who can add, edit, and delete profile information and start, submit, and validate reports.
Credit Union Service Organization Registry (CUSO Registry)
[redacted]

Account Management
Leverages the GSS infrastructure access control and CUSO Registry application-level (system specific) controls.
[redacted]
[redacted]
[redacted] access enforcement based on the account type and the user logged into the account.
Separation of Duties
[redacted] outlines the procedures for separation of duties of CUSO Registry [redacted]
Least Privilege
[redacted]
[redacted] to only those functions necessary to perform the tasks for the assigned role.

- Table C3 below includes information on systems a third-party (contractor or other Federal agency) owns, operates, and/or manages on NCUA's behalf that processes, stores, or transmits NCUA information. During our annual FISMA audits, we do not independently assess whether NCUA's external providers' security controls (including access controls) meet Federal requirements. We assess NCUA's *oversight* of externally-provided systems. However, to address this response we queried NCUA system owner points of contact to obtain specific access control information on each of these systems, specifically: (1) the mechanism for authenticating to each systems (single factor or multi-factor) and (2) specific security configuration parameters. We included this information in the table.

Federal Standard:

- NIST 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life Cycle Approach* (February 2010) indicates: (1) Organizations are responsible and accountable for the risk incurred by use of services provided by external providers and address this risk by implementing compensating controls when the risk is greater than the authorizing official or the organization is willing to accept; (2) FISMA and OMB policy require external providers handling federal information or operating information systems on behalf of the federal government to meet the same security requirements as federal agencies; and (3) federal organizations are responsible for implementing the risk management framework's security authorization step for externally-provided systems unless the external provider is a federal agency.[8]

  - During our FISMA 2015 audit, we did not identify any concerns with NCUA's oversight of its external system providers.

Table C3: Third Party "Covered Systems" – Limited Access Controls Information

BudgetPak (Contractor System)	
Authentication	
[redacted]	[redacted]
Access Controls	
[redacted]	
[redacted]	
Security Configuration Parameters	
Parameter	**Setting**
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[8] If the external provider is a federal agency, the provider can conduct all risk management framework tasks to include the information system authorization.

[redacted]	[redacted]
[redacted]	[redacted]

Comprehensive Human Resources Integrated System (CHRIS) (Federal System)

Authentication

[redacted]	[redacted]

Access Controls

[redacted]

Security Configuration Parameters

Parameter	Setting
[redacted]	[redacted]

Concur Travel and Expense (Contractor System)

Authentication

[redacted]	[redacted]

Access Controls
[redacted]

Security Configuration Parameters	
Parameter	**Setting**
[redacted]	[redacted]

CyberGrants (Contractor System)

Authentication	
[redacted]	[redacted]

Access Controls
[redacted]

Security Configuration Parameters	
Parameter	**Setting**
[redacted]	[redacted]

Delphi (Federal System)

Authentication

[redacted]

Access Controls

[redacted]

Security Configuration Parameters

Parameter	Setting
[redacted]	[redacted]

Electronic Official Personnel Folder (eOPF) (Federal System)

Authentication

[redacted]

Access Controls

[redacted]

Security Configuration Parameters	
Parameter	**Setting**
[redacted]	[redacted]
Electronic Performance Management System (ePerformance) (Contractor System)	
Authentication	
[redacted]	[redacted]
Access Controls	
[redacted]	
Security Configuration Parameters	
Parameter	**Setting**
[redacted]	[redacted]
Employee Express (Federal System)	
Authentication	
[redacted]	[redacted]

Access Controls
[redacted]

Security Configuration Parameters	
Parameter	**Setting**
[redacted]	[redacted]

Employees' Compensation Operations and Management Portal (Federal System)

Authentication	
[redacted]	[redacted]

Access Controls
[redacted]

Security Configuration Parameters	
Parameter	**Setting**
[redacted]	[redacted]

Financial Disclosure Management (FDM) (Federal System)

Authentication	
[redacted]	[redacted]

[redacted]	
Access Controls	
[redacted]	
Security Configuration Parameters	
Parameter	**Setting**
[redacted]	
FOIAXpress (Contractor System)	
Authentication	
[redacted]	
Access Controls	
[redacted]	
Security Configuration Parameters	
Parameter	**Setting**
[redacted]	

[redacted]	[redacted]
Integrity (Federal System)	
Authentication	
[redacted]	[redacted]
Access Controls	
[redacted]	
Security Configuration Parameters	
Parameter	**Setting**
[redacted]	[redacted]

[9] Federal Risk and Authorization Management Program (FedRAMP) is the government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. A cloud system is compliant with FedRAMP if it meets the following requirements: (a) The system security package has been created using the required FedRAMP templates; (b) The system meets the FedRAMP security control requirements; (c) The system has been assessed by an independent assessor; (d) A Provisional Authorization, and/or an Agency ATO, has been granted for the system; and (e) An authorization letter for the system is on file with the FedRAMP Program Management Office (PMO).

Micropact i-complaints® EEO/RA case management (Contractor System)	
Authentication	
[redacted]	[redacted]
Access Controls	
[redacted]	
[redacted]	
The i-complaints® system is part of the MicroPact Product Suite, which is FedRAMP compliant.	
[redacted]	
Security Configuration Parameters	
Parameter	**Setting**
[redacted]	[redacted]

NCUA LearnCenter (Contractor System)	
Authentication	
[redacted]	[redacted]
Access Controls	
[redacted]	
[redacted]	

[redacted]

Security Configuration Parameters	
Parameter	**Setting**
[redacted]	[redacted]

Pay.gov (Federal System)

Authentication	
[redacted]	[redacted]

Access Controls

[redacted]

Security Configuration Parameters	
Parameter	**Setting**
[redacted]	[redacted]

Personnel and Security System (PASS) (Contractor System)	
Authentication	
[redacted]	[redacted]
Access Controls	
[redacted]	
[redacted]	
[redacted]	
[redacted]	
Security Configuration Parameters	
Parameter	**Setting**
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Salesforce (Contractor System)	
Authentication	
[redacted]	[redacted]

Access Controls
Salesforce is a FedRAMP-compliant cloud-based system.
[redacted]
[redacted]

Security Configuration Parameters	
Parameter	**Setting**
[redacted]	[redacted]

Send Word Now (Contractor System)

Authentication	
Logical Access Authentication	Single-Factor Authentication - User ID and Password

Access Controls
Send Word Now is a cloud service provider working with the government through the FedRAMP Security Assessment Framework and pursuing an Agency Authorization for the system. ("FedRAMP In Process")
[redacted]
[redacted]

Security Configuration Parameters	
Parameter	**Setting**
[redacted]	[redacted]

USAccess: Identity, Credentials, and Access Management Hewlett Packard Enterprise Assured Identity (GSA-Managed Contractor System[10])

Authentication	
[redacted]	[redacted]

Access Controls
[redacted]

Security Configuration Parameters	
Parameter	**Setting**
[redacted]	[redacted]

[10] The GSA HSPD-12 Managed Service Office (MSO) is the executive agent responsible for managing government-wide acquisition of information technology to implement HSPD-12 services. The GSA HSPD-12 MSO established the USAccess program as an efficient way for federal agencies to issue common HSPD-12 approved credentials to their employees and contractors.

B. A description and list of the logical access controls and multi-factor authentication used by the covered agency to govern access to covered systems by privileged users.

- NCUA-owned "Covered Systems." Domain administrators within NCUA's GSS have two separate accounts – one account is for *non-privileged* access to the normal network account and the other account is for *privileged* domain access.

[redacted]

- Third-Party "Covered Systems." [redacted]

C. If the covered agency does not use logical access controls or multi-factor authentication to access a covered system, a description of the reasons for not using such logical access controls or multi-factor authentication.

- NCUA-owned "Covered Systems." As described in Table C1 above, NCUA uses logical access controls, which follow Federal standards except where indicated. [redacted] have adversely impacted the agency's business operations considering that the

[redacted]

- Third-Party "Covered Systems." We cannot attest to the logical access controls of NCUA's third-party systems'. However, we have assessed NCUA's compliance with NIST 800-37 as part of our FISMA audits as indicated in response to "A." above. Therefore, as of the FISMA 2015 reporting period, we can assert that NCUA has followed the appropriate Risk Management Framework guidelines to authorize the operation of these third-party systems within its Information Technology environment and to explicitly accept the risk(s) to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

D. A description of the following information security management practices used by the covered agency regarding covered systems.

(i) The policies and procedures followed to conduct inventories of the software present on the covered systems of the covered agency and the licenses associated with such software.

(ii) What capabilities the covered agency utilizes to monitor and detect exfiltration and other threats, including—

(I) Data loss prevention capabilities;

- NCUA informed us it acquired the [redacted] for its data loss prevention (DLP) capabilities.

(II) Forensics and visibility capabilities;

- NCUA indicates it uses [redacted]
- NCUA informed us it uses [redacted]

(III) Digital rights management capabilities.

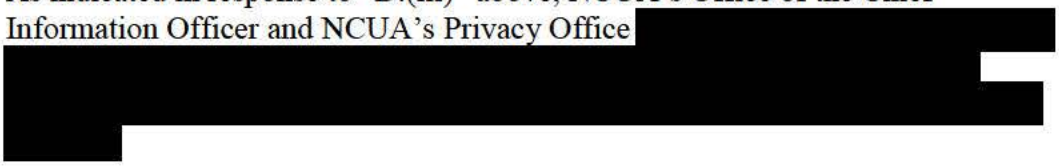
- NCUA informed us it is in the process of conducting research/analysis for potential Digital Rights Management (DRM) solutions and methodologies. [redacted]

(iii) A description of how the covered agency is using the capabilities described in clause (ii).

- NCUA informed us it is testing the "discovery" mode of its DLP solution. NCUA indicated it has set the discovery mode to identify where social security numbers are located throughout the network. NCUA's Office of the Chief Information Officer is working with NCUA's Privacy Office to establish appropriate parameters for maturing the testing into a holistic solution to address people, process, and technology requirements to ensure an effective DLP Program.
- NCUA indicated it uses [redacted]

- NCUA informed us it uses 

(iv) If the covered agency is not utilizing capabilities described in clause (ii), a description of the reasons for not utilizing such capabilities.

- As indicated in response to "D.(iii)" above, NCUA's Office of the Chief Information Officer and NCUA's Privacy Office 

- NCUA informed us that implementing an effective DLP and DRM program requires the agency to categorize and label data, define policies/processes that protect sensitive information, and develop business processes for operating and maintaining the collection program/solution.

E. A description of the policies and procedures of the covered agency with respect to ensuring that entities, including contractors, that provide services to the covered agency are implementing the information security management practices described in subparagraph (D).

- All users (including Managers, Senior Executives, and contractors) receive security awareness training when accessing NCUA information systems or when required by information system changes.
  - NCUA makes new employees aware of NCUA's information security requirements during the new hire orientation process. In addition, NCUA requires new employees to complete NCUA General Security Awareness Training within 10 business days of their Entry on Duty date.
  - NCUA requires existing users (employees and contractors) to complete annual security awareness refresher training.
- NCUA provides role-based security training annually to individuals with the following responsibilities directly related to securing information assets:
  - Chief Information Security Officer (CISO)

  - Information Systems Security Officer (ISSO)
  - Programmers/Developers
  - Database Administrators
  - Database Operators
  - System Administrators
  - Network Administrators
  - Help Desk Personnel

- NCUA has agency policy and procedures requiring information security and privacy requirements be included in vendor contracts.

  - NCUA's *Information Security Language for Information Technology Acquisitions* (March 2, 2016) provides current IT security and privacy requirements to ensure federally mandated security and privacy controls and standards are met within the Agency. NCUA indicated it requires the use of specific contract language when any of the following conditions apply:

    - Whenever any contractor (and/or any subcontractor) employee will develop, have the ability to access, or host and/or maintain federal information and/or federal information system(s).

    - Whenever any contractor (and/or any subcontractor) employee will access, or use, Personally Identifiable Information (PII), including instances of remote access to or physical removal of such information beyond agency premises or control.

    - Whenever any contractor (and/or any subcontractor) employee will have regular or prolonged physical access to a "federally-controlled facility," as defined in FAR Subpart 2.1.

    - Whenever cloud-based services will be acquired.

  - A statement on Information Security Requirements applies whenever a contract includes one or both of the following:

    - A contractor (and/or any subcontractor) employee will have, or the ability to have, physical or logical (electronic) access to federal information.

    - A contractor (and/or any subcontractor) will operate a federal information technology system containing information that directly supports the NCUA mission.

- Following are the requirements for Information Security Awareness Training:

  - All contractor (and/or any subcontractor) employees shall complete the applicable mandatory NCUA Information Security Awareness training before performing any work under this contract. Thereafter, the employees shall complete this training annually, during the life of this contract.

  - The contractor (and/or any subcontractor) shall maintain training records for all information security awareness and role-based training completed by each employee working under this contract. The training records shall be provided to the Contracting Officer's Representative (COR) and/or Contracting Officer in conjunction with contract award or upon request and any program office specific rules, as applicable.

  - The contractor shall provide records of any applicable information security awareness and role-based training completed outside of NCUA/ program office to the COR responsible for their contract.

- Following are the requirements for NCUA's Rules of Behavior:

  - The contractor (and/or any subcontractor) shall ensure that all employees comply with the NCUA Information Technology General Rules of Behavior and any program office specific rules, as applicable.

  - All contractor employees must read and adhere to the Rules of Behavior before accessing Agency data or other information, systems, and/or networks that store/process NCUA information and annually thereafter.