



August 10, 2016

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

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

The Honorable Thomas R. Carper  
Ranking Member  
Committee on Homeland Security and  
Governmental Affairs  
United States Senate  
328 Hart Senate Office Building  
Washington, DC 20510

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

Dear Honorable Chairmen and Ranking Members:

The Cybersecurity Act of 2015, Sec 406 (b), requires each Office of Inspector General (OIG) to submit to the appropriate committees of jurisdiction in the Senate and the House of Representatives a report that contains information regarding its agency's policies, practices, and controls related to logical access, multi-factor authentication, privileged users, software inventory and license management, and exfiltration.

We are completing this work in conjunction with our annual Federal Information Security Modernization Act (FISMA) evaluations from 2015 and 2016. This report incorporates results from our [2015 FISMA evaluation](#) report which is available on our website. Additional information will be provided in our 2016 FISMA evaluation report.

The following contains the requested information from Sec 406 (b) and a description of the Farm Credit Administration's (FCA) policies, practices, and related controls:

*(A) A description of the logical access<sup>1</sup> policies and practices used by the covered agency to access a covered system, including whether appropriate standards were followed.*

---

<sup>1</sup> "logical access control" means a process of granting or denying specific requests to obtain and use information and related information processing services

**FCA OIG response:**

The logical access policies and practices used by FCA include:

- Documented policies and procedures related to logical access controls, including requesting, issuing, and closing information system accounts
- Network access provided after the employee certifies they have read the agency's policy on information security
- Identification and authentication of information system users before allowing access
- Detection of unauthorized devices and disabling connectivity
- Dual factor authentication
- Information system accounts created, managed, monitored, and disabled by authorized personnel
- User access based on separation of duties controlled through group and permissions
- Complex password policy with periodic password change required
- Lockout after a predefined amount of unsuccessful login attempts
- Re-authentication after period of inactivity
- Periodic review of information system accounts to ensure access permissions provided to users are current and approved
- Controls to prevent, detect, or notify authorized personnel of suspicious activity or devices
- Annual security awareness training and periodic security awareness articles
- Controls over remote and wireless access

Routine testing of compliance with policies, procedures, FISMA requirements, Office of Management and Budget (OMB) policy, and applicable National Institute of Standards and Technology (NIST) guidelines includes:

- Self-evaluations by Technology and Governance Divisions
- Penetration tests performed by independent contractors
- Evaluation of security requirements by independent contractors
- Annual OIG FISMA evaluations

Any weaknesses identified during testing were reported to the Chief Information Officer (CIO) and Governance Division for remediation.

*(B) A description and list of the logical access controls and multi-factor authentication<sup>2</sup> used by the covered agency to govern access to covered systems by privileged users<sup>3</sup>.*

**FCA OIG response:**

In addition to the logical access policies and practices for non-privileged accounts listed above, FCA has the following additional controls for privileged access:

- Privileged accounts are limited to FCA employees required to have elevated access privileges

---

<sup>2</sup> "multifactor authentication" means the use of not fewer than 2 authentication factors

<sup>3</sup> "privileged user" means a user who has access to system control, monitoring, or administrative functions

- Prior to considering elevated access, a potential privileged user must be trained, demonstrate the skills required for elevated access, and be approved by the Technology Division administrators and CIO
- Privileged users maintain two accounts and the privileged account is only used when necessary
- Privileged accounts require a 2<sup>nd</sup> smartcard
- The number of privileged accounts was reduced during the Cybersecurity Sprint
- Privileges are reviewed periodically
- Privileged accounts are monitored through alerts
- Temporary local administrator privileges are generally scheduled to be revoked the same day and informed about the use and risk of these privileges

*(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.*

**FCA OIG response:**

FCA uses logical access controls, including multi-factor authentication, to access covered systems as described above in (A) and (B).

*(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.*

**FCA OIG response:**

FCA has policies and procedures for inventorying software and licenses. FCA has the capability to perform routine inventories of software and conducts an annual software inventory using an automated tool. Software licenses and their respective agreements are reviewed during the annual budget cycle and at license renewal.

Workstations are pre-loaded with a standard software configuration. There is a policy prohibiting users from installing non-standard software on their workstation without approval by the CIO. This policy is enforced by technical settings which prevent users from installing software.

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

*(I) data loss prevention capabilities;*

**FCA OIG response:**

FCA has various data loss prevention capabilities including the following:

- Logical access controls that limit access to and enforce separation of duties
- Various types of encryption
  - Workstations with total drive encryption
  - Encrypted virtual private network (VPN) traffic
  - Encrypted backups
  - Secure webmail
  - Forced encryption of removable USB devices
  - Encryption of sensitive data
- Tools that have the capability of preventing emails or data with sensitive financial information from transmission
  - An intrusion prevention system that can monitor and control data transfers
  - An anti-spam email and filtering appliance that has the capability to prevent sending emails with social security numbers and credit card numbers
  - A suite of productivity software that has the capability of flagging financial data such as credit card numbers and account numbers
  - A firewall with data loss prevention capabilities
- Users are prohibited from writing data to DVD and CD without approval from the CIO
- Signed agreements with the Department of Homeland Security (DHS) for intrusion detection and prevention systems

(II) *forensics and visibility capabilities; or*

**FCA OIG response:**

FCA has various forensics and visibility capabilities including the following:

- Multiple intrusion prevention and detection systems with anti-virus, anti-spam, firewall, device control, and web filtering, with reporting and log capabilities
- Signed agreements with DHS for continuous monitoring and incident response capabilities
- Signed agreement with DHS for forensic and visibility capabilities
- Vulnerability scans
- Email notifications for various types of security events
- Tool for performing forensic backups
- Various system logs and reports

(III) *digital rights management capabilities.*

**FCA OIG response:**

Sensitive agency information is protected by general controls including the logical access controls described above from unauthorized review, distribution, and modification.

Additionally, FCA has the following tools that have the capability of adding an additional layer of digital rights management protection to sensitive documents and data:

- Productivity software that has the ability to restrict permissions to print, forward, or copy sensitive information
- Digital document workflow software with the ability to protect a document with a password or prevent others from copying and editing the document

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

(I) *data loss prevention capabilities;*

**FCA OIG response:**

FCA has implemented the following data loss prevention capabilities:

- Logical access controls that limit access to and enforce separation of duties
- Various types of encryption are used to protect sensitive data at rest and in transit
  - Workstations with total drive encryption
  - Encrypted VPN traffic
  - Encrypted backups
  - Secure webmail
  - Forced encryption of removable USB devices
  - Encryption for sensitive data
- Users are prohibited from writing data to DVD and CD without approval from the CIO
- Signed agreements with DHS for intrusion detection and prevention systems that include active monitoring of FCA systems

(II) *forensics and visibility capabilities; or*

**FCA OIG response:**

FCA has implemented the following forensics and visibility capabilities:

- Multiple intrusion prevention and detection systems with anti-virus, anti-spam, firewall, device control, and web filtering, with reporting and log capabilities
- Signed agreements with DHS for continuous monitoring and incident response capabilities
- Signed agreement with DHS for forensic and visibility capabilities
- Vulnerability scans
- Email notifications for various types of security events
- Various system logs and reports

(III) digital rights management capabilities.

**FCA OIG response:**

Sensitive agency information is protected by general controls including the logical access controls described above from unauthorized review, distribution, and modification.

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

(I) data loss prevention capabilities;

**FCA OIG response:**

FCA has not implemented the following data loss prevention capabilities:

- Tools that have the capability of preventing emails or data with sensitive financial information from transmission
  - An intrusion prevention system that can monitor and control data transfers
  - An anti-spam email and filtering appliance that has the capability to prevent sending emails with social security numbers and credit card numbers
  - A suite of productivity software that has the capability of flagging financial data such as credit card numbers and account numbers
  - A firewall with data loss prevention capabilities

FCA is in the process of obtaining an independent contractor to perform a complete assessment of its information security program and improve the risk assessment process. FCA plans to weigh the benefit of these capabilities with the resources needed as part of its risk management process. The Office of Information Technology created a project to evaluate data loss prevention tools and develop an implementation plan.

(III) digital rights management capabilities.

**FCA OIG response:**

FCA has the following tools that have the capability of adding an additional layer of digital rights management protection to sensitive documents and data but have not been implemented:

- Productivity software
- Digital document workflow software

FCA is in the process of obtaining an independent contractor to perform a complete assessment of its information security program and improve the risk assessment process. FCA plans to weigh the benefit of these capabilities with the resources needed as part of its risk management process.

*(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).*

**FCA OIG response:**

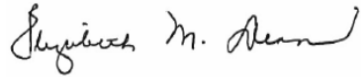
FCA uses a combination of contractor systems and individual contractors to support its operations.

FCA has established and maintains a program to oversee systems operated on its behalf by contractors. FCA has documented policies and procedures. Contractor systems and interconnections have written agreements, memorandums of understanding, interconnection agreements, or contracts. Security plans have been documented and updated annually for the financial, personnel, and payroll systems. FCA also monitors the security controls for the outsourced systems and performs due diligence reviews and access control reviews.

FCA has policies and procedures for the onboarding of individual contractors which include background investigations, written agreements, confidentiality agreements, and security awareness training. Before gaining access to agency systems, individual contractors are required to certify they have read and understand FCA's information security policies and procedures.

Thank you for your efforts on behalf of the Inspectors General, and please contact my office at (703) 883-4030, if we may further assist.

Sincerely,



Elizabeth M. Dean  
Inspector General

cc: The Honorable Pat Roberts  
Chairman  
Committee on Agriculture, Nutrition and Forestry  
United States Senate

The Honorable Debbie Stabenow  
Ranking Member  
Committee on Agriculture, Nutrition and Forestry  
United States Senate

The Honorable K. Michael Conaway  
Chairman  
Committee on Agriculture  
United States House of Representatives

The Honorable Collin C. Peterson  
Ranking Member  
Committee on Agriculture  
United States House of Representatives