OFFICE OF

INSPECTOR GENERAL

Report of Evaluation

OIG 2013 Evaluation of the
Farm Credit Administration's
Compliance with the
Federal Information Security
Management Act

November 19, 2013

E-13-01

Tammy Rapp
Auditor-in-Charge

FARM CREDIT ADMINISTRATION

Memorandum

Office of Inspector General
1501 Farm Credit Drive
McLean, Virginia 22102-5090

November 19, 2013

The Honorable Jill Long Thompson, Board Chair and Chief Executive Officer
The Honorable Kenneth A. Spearman, Board Member
The Honorable Leland A. Strom, Board Member
Farm Credit Administration
1501 Farm Credit Drive
McLean, Virginia 22102-5090

Dear Board Chair Long Thompson and FCA Board Members Spearman and Strom:

The Office of the Inspector General completed the 2013 independent evaluation of the Farm Credit Administration's compliance with the Federal Information Security Management Act (FISMA). The objectives of this evaluation were to perform an independent assessment of FCA's information security program and assess FCA's compliance with FISMA.

The results of our evaluation revealed that FCA has an effective information security program. However, the Agency agreed to make improvements in two areas.

We appreciate the courtesies and professionalism extended to the evaluation staff. If you have any questions about this evaluation, I would be pleased to meet with you at your convenience.

Respectfully,

Elizabeth M. Dean
Inspector General

Office of Inspector General Evaluation of the Farm Credit Administration's Compliance with the Federal Information Security Management Act 2013

Report #E-13-01

Farm Credit Administration
Office of Inspector General

November 19, 2013

OIG Evaluation: FISMA 2013

- Introduction and Background
- Objectives, Scope, and Methodology
- Overall Conclusion
- Areas Evaluated by Offices of Inspector General (OIG) During FY2013
  1. Continuous Monitoring Management
  2. Configuration Management
  3. Identity and Access Management
  4. Incident Response and Reporting
  5. Risk Management
  6. Security Training
  7. Plans of Action and Milestones (POA&M)
  8. Remote Access Management
  9. Contingency Planning
  10. Contractor Systems
  11. Security Capital Planning
- Appendix A: IG Section Report for Office of Management and Budget (OMB)

Introduction and Background

- The President signed into law the E-Government Act (Public Law 107-347), which includes Title III, Information Security, on December 17, 2002. Title III permanently reauthorized the Government Information Security Reform Act of 2000 and renamed it the Federal Information Security Management Act (FISMA) of 2002. The purpose of FISMA was to strengthen the security of the Federal government's information systems and develop minimum standards for agency systems.
- FISMA requires an agency's Chief Information Officer (CIO) and OIG to conduct annual assessments of the agency's information security program.
- In the past, OMB issued a memorandum with annual reporting instructions for complying with FISMA's annual reporting requirements and reporting on the agency's privacy management program. However, as of November 8, 2013, OMB had not issued reporting instructions for FY 2013, so we relied on OMB's FY 2012 instructions and announcements posted on the CyberScope Home Page.
- Results of the CIO and OIG assessments are reported to the OMB thru CyberScope.
- Appendix A contains the IG Section Report as submitted to OMB thru CyberScope.

Objectives, Scope, and Methodology

- The objectives of this evaluation were to perform an independent assessment of the Farm Credit Administration's (FCA or Agency) information security program and assess FCA's compliance with FISMA.
- The scope of this evaluation covered FCA's Agency-owned and contractor operated information systems of record as of September 30, 2013. FCA is a single program Agency with nine mission critical systems and major applications.
- The evaluation covered the eleven areas identified by Department of Homeland Security (DHS) for OIGs to evaluate.
- Key criteria used to evaluate FCA's information security program and compliance with FISMA included OMB guidance, National Institute of Standards and Technology (NIST) Special Publications (SP), and Federal Information Processing Standards Publications (FIPS).
- In performing this evaluation, we performed the following steps:
  - Identified and reviewed Agency policies and procedures related to information security;
  - Examined documentation relating to the Agency's information security program and compared to NIST standards and FCA policy;
  - Conducted interviews with the CIO, Information Technology (IT) Security Specialist, Technology Team Leader, Applications Team Leader, and several IT Specialists;
  - Built on our understanding from past FISMA evaluations;
  - Observed security related activities performed by Agency personnel; and
  - Performed tests for a subset of controls.

Objectives, Scope, and Methodology

- This evaluation represents the status of the information security program as of September 30, 2013, and did not include a test of all information security controls.
- The evaluation was performed at FCA Headquarters in McLean, Virginia, from September 2013 through November 2013.
- Observations and results were shared with key IT personnel throughout the evaluation. On November 12, 2013, the CIO and OIG shared and discussed drafts of their respective FISMA section reports.
- An exit conference was conducted with management officials on November 12, 2013.
- This evaluation was performed in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*.

Overall Conclusion

FCA has an effective information security program that continues to mature and contains the following elements:

- Information security policies and procedures
- Continuous monitoring
- Standard baseline configurations
- Identity and access management program
- Incident response program
- Risk based approach to information security
- Systems categorized based on risk
- Risk based security controls implemented
- Security authorization process
- Security awareness and training program
- Developing plans and implementing corrective action for significant information security weaknesses
- Remote access controls
- Continuity of operations plan and tests
- Oversight of contractor systems
- Capital planning and investment process that incorporates information security requirements

Overall Conclusion

- FCA's CIO and experienced IT team are proactive in their approach to information security
- The IT team and system sponsors were responsive to suggestions made for improvement during the FISMA evaluation and, in many cases, the IT staff made immediate changes to strengthen the information security program
- Of the 11 areas OMB required OIGs to evaluate during 2013, FCA has established a program in each of the areas that is consistent with NIST's and OMB's guidelines.
- However, we identified two areas where improvements need to be made which resulted in two agreed-upon actions:
  1. Periodically review permissions for a major application
  2. Strengthen oversight of an outsourced system (See slide 10 and 17)

Continuous Monitoring Management

The Agency has established an enterprise-wide continuous monitoring program that assesses the security state of information systems that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. The continuous monitoring program includes the following attributes:

- Continuous monitoring strategy reflected in security plans
- Malicious code protection
- Vulnerability scanning
- Log monitoring
- Notification of unauthorized devices
- Notification of changes or additions to sensitive accounts
- Ongoing monitoring of security alerts and updates from vendors and appropriate action
- Commitment to annual independent penetration test

Configuration Management

The Agency established and is maintaining a configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. FCA's security configuration management program includes the following attributes:

- Documented policies and procedures for configuration management
- Standard baseline configuration for workstations and servers
- Implementation of the United States Government Configuration Baseline (USGCB)
- Regular scanning of servers for vulnerabilities and compliance within the baseline configuration
- Controls to prevent unauthorized software
- Controls to prevent unauthorized devices
- Timely remediation of identified vulnerabilities
- Process for timely and secure installation of software patches
- Monitoring and analysis of critical security alerts to determine potential impact to FCA systems

Identity and Access Management

The Agency has established and is maintaining an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. The account and identity management program identifies users and network devices and includes the following attributes:

- Documented policies and procedures for requesting, issuing, and closing information system accounts
- Identifies and authenticates information system users before allowing access
- Detects unauthorized devices and disables connectivity
- Dual-factor authentication
- Strengthened controls over use of elevated privileges
- Information system accounts created, managed, monitored, and disabled by authorized personnel
- Periodic review of information system accounts to ensure access permissions provided to users is current and appropriate. However, permissions to a major application needs to be reviewed to ensure access is limited to authorized users.
- Controls to prevent, detect, or notify authorized personnel of suspicious account activity or devices

Agreed-upon Action:

1. OMS will facilitate a review of permissions to a major application to ensure access is limited to authorized users.

Incident Response and Reporting

The Agency has established and is maintaining an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. The incident response and reporting program includes the following attributes:

- Documented policies and procedures, security awareness training and articles, and a 24 hour Helpline for incidents available to employees needing incident assistance.
- Agency staff must report within one hour to the OMS Helpline any IT equipment, personally identifiable information (PII), or sensitive information that is suspected to be missing, lost, or stolen.
- During FY 2013, FCA had the following types of incidents:
  - Power outage and halon discharge in the computer room
  - Voluminous spam received via the website
  - Malware on laptops
  - Unauthorized computers detected and removed from FCA's network
  - Unauthorized scans and attempted unauthorized access blocked from FCA's network
  - Phishing email attempts
  - Misplaced or lost HSPD12 cards and smart phones (Some lost phones and cards were recovered.)
- Analysis was performed for each incident before responding appropriately and timely to minimize further damage.
- A log was maintained of security incidents, and appropriate officials were notified depending on the nature of the incident.

Risk Management

FCA established and maintained a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. The risk management program includes the following attributes:

- Policy that general support system and major applications will operate with proper accreditation and undergo reauthorization every 3 years or when a major system change occurs
- Addresses risk from organization, mission, business, and information system perspectives
- Information systems categorized based on FIPS 199 and SP 800-60
- Security plans based on risk that identify minimum baseline controls selected, documented, and implemented
- Periodic assessments of controls through a combination of continuous monitoring, self-assessments, independent penetration tests, and independent security tests and evaluations
- Authorizing official considers items identified during the certification process before signing the "Authorization to Operate"
- Regular communications with senior management

Security Training

The Agency has established and is maintaining a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. The security training program includes the following attributes:

- Mandatory annual security awareness training for employees and contractors using small group sessions
  - Protecting PII and sensitive information
  - Standardized hardware and software
  - Using the internet and e-mail
  - Web security appliance
- Security training presentation at new employee orientation
- New employees and contractors required to certify they have read and understood FCA's computer security policies and responsibilities after briefing by the IT Security Specialist
- Ongoing awareness program that includes e-mails and news alerts with security tips and notices of new threats
- Individual development plan (IDP) process used to identify specialized training for users with significant security responsibilities
- Identification and tracking of employees requiring mandatory security training

Plans of Action & Milestones (POA&M)

The Agency has established and is maintaining a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. The POA&M program tracks and monitors known information security weaknesses and includes the following attributes:

- Policy for developing plans of action and milestones
- Process for developing plans of corrective action for significant information security weaknesses and tracking their implementation
- Compensating controls currently in place until outstanding items are remediated

Remote Access Management

The Agency has established and is maintaining a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. The remote access program includes the following attributes:

- Policies and procedures for authorizing, monitoring, and controlling all methods of remote access
- Protection against unauthorized connections
- Virtual private network (VPN) for secure encrypted transmission of data outside of the Agency's network
- Encryption on local hard drives and USB drives to protect sensitive data and PII
- Forced encryption when creating CDs and DVDs
- Security policy and device management for Agency smart phones and authorized personal devices
- Remote contractor access for diagnostic purposes tightly controlled and closely supervised by IT staff

Contingency Planning

The Agency established and is maintaining an enterprise-wide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. The contingency planning program includes the following attributes:

- Business continuity plan and disaster recovery plan periodically updated to support the restoration of operations and systems after a disruption or failure
- Alternative processing site and essential systems successfully activated during a government wide test
- Backup strategy includes daily and weekly backups of data and systems
- Off-site storage and encryption for backups
- Disaster recovery kit maintained offsite that contains critical software needed to recreate systems
- Employee notification system used to alert employees of office closings and other events

Contractor Systems

The Agency has established and maintains a program to oversee systems operated on its behalf by contractors or other entities, including Agency systems and services residing in the cloud external to the Agency. The contractor system oversight program includes the following attributes:

- Obtained written agreements for contractor systems and interconnections
- Updated inventory of contractor systems and interconnections annually
- Reviewed and updated security plans for contractor systems annually
- Performed due diligence reviews and monitored security controls for the outsourced financial and payroll systems, but needs to improve oversight of the outsourced electronic official personnel folder (eOPF) system
- Performed site visits to review security documentation and verify financial system providers employed adequate security measures to protect data, applications, and services
- Periodically reviewed user accounts and privileges for outsourced financial and payroll systems. However, OMS agreed to increase the frequency of access control reviews for the outsourced payroll and eOPF systems.

Agreed-upon Action:

2. OMS will strengthen oversight of the outsourced eOPF system:
   a) Clearly define controls in the security plan including frequency of review and responsible party
   b) Periodically review access control lists to ensure access is appropriate and limited to authorized users
   c) Obtain and review independent security assessment report regarding security of the system.

Security Capital Planning

The Agency has established and maintains a security capital planning and investment program for information security. The program includes the following attributes:

- Policies and procedures that stress importance of information security and protecting sensitive information
- Capital planning and investment process that incorporates information security requirements
- Enterprise architecture that ensures IT investments support core business functions and provides security standards
- Information security resources are available as planned

Inspector General

Section Report

2013

Annual FISMA Report

Farm Credit Administration

Section 1: Continuous Monitoring Management

1.1 **Has the organization established an enterprise-wide continuous monitoring program that assesses the security state of information systems that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?**

Yes

1.1.1 **Documented policies and procedures for continuous monitoring (NIST SP 800-53: CA-7).**

Yes

1.1.2 **Documented strategy and plans for continuous monitoring (NIST SP 800-37 Rev 1, Appendix G).**

Yes

1.1.3 **Ongoing assessments of security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans (NIST SP 800-53, NIST 800-53A).**

Yes

1.1.4 **Provides authorizing officials and other key system officials with security status reports covering updates to security plans and security assessment reports, as well as a common and consistent POA&M program that is updated with the frequency defined in the strategy and/or plans (NIST SP 800-53, 800-53A).**

Yes

1.2 **Please provide any additional information on the effectiveness of the organization's Continuous Monitoring Management Program that was not noted in the questions above.**

See OIG evaluation report for additional information.

Section 2: Configuration Management

2.1 **Has the organization established a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?**

Yes

2.1.1 **Documented policies and procedures for configuration management.**

Yes

2.1.2 **Defined standard baseline configurations.**

Yes

Section 2: Configuration Management

2.1.3 Assessments of compliance with baseline configurations.

Yes

2.1.4 Process for timely, as specified in organization policy or standards, remediation of scan result deviations.

Yes

2.1.5 For Windows-based components, USGCB secure configuration settings are fully implemented, and any deviations from USGCB baseline settings are fully documented.

Yes

2.1.6 Documented proposed or actual changes to hardware and software configurations.

Yes

2.1.7 Process for timely and secure installation of software patches.

Yes

2.1.8 Software assessing (scanning) capabilities are fully implemented (NIST SP 800-53: RA-5, SI-2).

No

Comments: Servers are periodically scanned for compliance with the baseline configuration. However, a risk based decision was made to not implement routine scanning of workstations for compliance with FCA's baseline configuration. A cost benefit analysis with consideration of compensating controls was an integral part of the decision.

2.1.9 Configuration-related vulnerabilities, including scan findings, have been remediated in a timely manner, as specified in organization policy or standards. (NIST SP 800-53: CM-4, CM-6, RA-5, SI-2)

Yes

2.1.10 Patch management process is fully developed, as specified in organization policy or standards. (NIST SP 800-53: CM-3, SI-2).

Yes

2.2 Please provide any additional information on the effectiveness of the organization's Configuration Management Program that was not noted in the questions above.

See OIG evaluation report for additional information.

Section 3: Identity and Access Management

Section 3: Identity and Access Management

3.1 Has the organization established an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and which identifies users and network devices? Besides the improvement opportunities that have been identified by the OIG, does the program include the following attributes?

Yes

3.1.1 Documented policies and procedures for account and identity management (NIST SP 800-53: AC-1).

Yes

3.1.2 Identifies all users, including Federal employees, contractors, and others who access organization systems (NIST SP 800-53, AC-2).

Yes

3.1.3 Identifies when special access requirements (e.g., multi-factor authentication) are necessary.

Yes

3.1.4 If multi-factor authentication is in use, it is linked to the organization's PIV program where appropriate (NIST SP 800-53, IA-2).

Yes

3.1.5 Organization has planned for implementation of PIV for logical access in accordance with government policies (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11).

Yes

3.1.6 Organization has adequately planned for implementation of PIV for physical access in accordance with government policies (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11).

Yes

3.1.7 Ensures that the users are granted access based on needs and separation-of-duties principles.

Yes

3.1.8 Identifies devices with IP addresses that are attached to the network and distinguishes these devices from users (For example: IP phones, faxes, printers are examples of devices attached to the network that are distinguishable from desktops, laptops or servers that have user accounts).

Yes

Section 3: Identity and Access Management

3.1.9 **Identifies all user and non-user accounts. (Refers to user accounts that are on a system. Data user accounts are created to pull generic information from a database or a guest/anonymous account for generic login purposes. They are not associated with a single user or a specific group of users.)**

Yes

3.1.10 **Ensures that accounts are terminated or deactivated once access is no longer required.**

Yes

3.1.11 **Identifies and controls use of shared accounts.**

Yes

3.2 **Please provide any additional information on the effectiveness of the organization's Identity and Access Management Program that was not noted in the questions above.**

See OIG evaluation report for additional information.

Comments: FCA periodically reviews security permissions for its general support system and most major applications. However, permissions for one major application need to be periodically reviewed to ensure access is limited to authorized users.

Section 4: Incident Response and Reporting

4.1 **Has the organization established an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?**

Yes

4.1.1 **Documented policies and procedures for detecting, responding to, and reporting incidents (NIST SP 800-53: IR-1).**

Yes

4.1.2 **Comprehensive analysis, validation and documentation of incidents.**

Yes

4.1.3 **When applicable, reports to US-CERT within established timeframes (NIST SP 800-53, 800-61, and OMB M-07-16, M-06-19).**

Yes

4.1.4 **When applicable, reports to law enforcement within established timeframes (NIST SP 800-61).**

Yes

Section 4: Incident Response and Reporting

4.1.5 Responds to and resolves incidents in a timely manner, as specified in organization policy or standards, to minimize further damage (NIST SP 800-53, 800-61, and OMB M-07-16, M-06-19).

Yes

4.1.6 Is capable of tracking and managing risks in a virtual/cloud environment, if applicable.

Yes

4.1.7 Is capable of correlating incidents.

Yes

4.1.8 Has sufficient incident monitoring and detection coverage in accordance with government policies (NIST SP 800-53, 800-61; OMB M-07-16, M-06-19).

Yes

4.2 Please provide any additional information on the effectiveness of the organization's Incident Management Program that was not noted in the questions above.

See OIG evaluation report for additional information.

Section 5: Risk Management

5.1 Has the organization established a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

Yes

5.1.1 Documented policies and procedures for risk management, including descriptions of the roles and responsibilities of participants in this process.

Yes

5.1.2 Addresses risk from an organization perspective with the development of a comprehensive governance structure and organization-wide risk management strategy as described in NIST SP 800-37, Rev.1.

Yes

5.1.3 Addresses risk from a mission and business process perspective and is guided by the risk decisions from an organizational perspective, as described in NIST SP 800-37, Rev. 1.

Yes

Section 5: Risk Management

5.1.4 Addresses risk from an information system perspective and is guided by the risk decisions from an organizational perspective and the mission and business perspective, as described in NIST SP 800-37, Rev. 1.

Yes

5.1.5 Has an up-to-date system inventory.

Yes

5.1.6 Categorizes information systems in accordance with government policies.

Yes

5.1.7 Selects an appropriately tailored set of baseline security controls.

Yes

5.1.8 Implements the tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation.

Yes

5.1.9 Assesses the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Yes

5.1.10 Authorizes information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.

Yes

5.1.11 Ensures information security controls are monitored on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.

Yes

5.1.12 Information-system-specific risks (tactical), mission/business-specific risks, and organizational-level (strategic) risks are communicated to appropriate levels of the organization.

Yes

Section 5: Risk Management

5.1.13 Senior officials are briefed on threat activity on a regular basis by appropriate personnel (e.g., CISO).

Yes

5.1.14 Prescribes the active involvement of information system owners and common control providers, chief information officers, senior information security officers, authorizing officials, and other roles as applicable in the ongoing management of information system-related security risks.

Yes

5.1.15 Security authorization package contains system security plan, security assessment report, and POA&M in accordance with government policies. (NIST SP 800-18, 800-37).

Yes

5.1.16 Security authorization package contains accreditation boundaries, defined in accordance with government policies, for organization information systems.

Yes

5.2 Please provide any additional information on the effectiveness of the organization's Risk Management Program that was not noted in the questions above.

See OIG evaluation report for additional information.

Section 6: Security Training

6.1 Has the organization established a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

Yes

6.1.1 Documented policies and procedures for security awareness training (NIST SP 800-53: AT-1).

Yes

6.1.2 Documented policies and procedures for specialized training for users with significant information security responsibilities.

Yes

6.1.3 Security training content based on the organization and roles, as specified in organization policy or standards.

Yes

Section 6: Security Training

6.1.4 **Identification and tracking of the status of security awareness training for all personnel (including employees, contractors, and other organization users) with access privileges that require security awareness training.**

Yes

6.1.5 **Identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other organization users) with significant information security responsibilities that require specialized training.**

Yes

6.1.6 **Training material for security awareness training contains appropriate content for the organization (NIST SP 800-50, 800-53).**

Yes

6.2 **Please provide any additional information on the effectiveness of the organization's Security Training Program that was not noted in the questions above.**

See OIG evaluation report for additional information.

Section 7: Plan Of Action & Milestones (POA&M)

7.1 **Has the organization established a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and tracks and monitors known information security weaknesses? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?**

Yes

7.1.1 **Documented policies and procedures for managing IT security weaknesses discovered during security control assessments and that require remediation.**

Yes

7.1.2 **Tracks, prioritizes and remediates weaknesses.**

Yes

7.1.3 **Ensures remediation plans are effective for correcting weaknesses.**

Yes

7.1.4 **Establishes and adheres to milestone remediation dates.**

Yes

Section 7: Plan Of Action & Milestones (POA&M)

7.1.5 Ensures resources and ownership are provided for correcting weaknesses.

Yes

7.1.6 POA&Ms include security weaknesses discovered during assessments of security controls and that require remediation (do not need to include security weakness due to a risk-based decision to not implement a security control) (OMB M-04-25).

Yes

7.1.7 Costs associated with remediating weaknesses are identified (NIST SP 800-53, Rev. 3, Control PM-3 and OMB M-04-25).

Yes

7.1.8 Program officials report progress on remediation to CIO on a regular basis, at least quarterly, and the CIO centrally tracks, maintains, and independently reviews/validates the POA&M activities at least quarterly (NIST SP 800-53, Rev. 3, Control CA-5; OMB M-04-25).

Yes

7.2 Please provide any additional information on the effectiveness of the organization's POA&M Program that was not noted in the questions above.

See OIG evaluation report for additional information.

Section 8: Remote Access Management

8.1 Has the organization established a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

Yes

8.1.1 Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access (NIST SP 800-53: AC-1, AC-17).

Yes

8.1.2 Protects against unauthorized connections or subversion of authorized connections.

Yes

8.1.3 Users are uniquely identified and authenticated for all access (NIST SP 800-46, Section 4.2, Section 5.1).

Yes

Section 8: Remote Access Management

8.1.4 Telecommuting policy is fully developed (NIST SP 800-46, Section 5.1).

Yes

8.1.5 If applicable, multi-factor authentication is required for remote access (NIST SP 800-46, Section 2.2, Section 3.3).

Yes

8.1.6 Authentication mechanisms meet NIST Special Publication 800-63 guidance on remote electronic authentication, including strength mechanisms.

Yes

8.1.7 Defines and implements encryption requirements for information transmitted across public networks.

Yes

8.1.8 Remote access sessions, in accordance with OMB M-07-16, are timed-out after 30 minutes of inactivity, after which re-authentication is required.

Yes

8.1.9 Lost or stolen devices are disabled and appropriately reported (NIST SP 800-46, Section 4.3, US-CERT Incident Reporting Guidelines).

Yes

8.1.10 Remote access rules of behavior are adequate in accordance with government policies (NIST SP 800-53, PL-4).

Yes

8.1.11 Remote access user agreements are adequate in accordance with government policies (NIST SP 800-46, Section 5.1, NIST SP 800-53, PS-6).

Yes

8.2 Please provide any additional information on the effectiveness of the organization's Remote Access Management that was not noted in the questions above.

See OIG evaluation report for additional information.

8.3 Does the organization have a policy to detect and remove unauthorized (rogue) connections?

Yes

Section 9: Contingency Planning

Section 9: Contingency Planning

9.1 Has the organization established an enterprise-wide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

Yes

9.1.1 Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster (NIST SP 800-53: CP-1).

Yes

9.1.2 The organization has incorporated the results of its system's Business Impact Analysis (BIA) into the analysis and strategy development efforts for the organization's Continuity of Operations Plan (COOP), Business Continuity Plan (BCP), and Disaster Recovery Plan (DRP) (NIST SP 800-34).

Yes

9.1.3 Development and documentation of division, component, and IT infrastructure recovery strategies, plans and procedures (NIST SP 800-34).

Yes

9.1.4 Testing of system specific contingency plans.

Yes

9.1.5 The documented BCP and DRP are in place and can be implemented when necessary (FCD1, NIST SP 800-34).

Yes

9.1.6 Development of test, training, and exercise (TT&E) programs (FCD1, NIST SP 800-34, NIST SP 800-53).

Yes

9.1.7 Testing or exercising of BCP and DRP to determine effectiveness and to maintain current plans.

Yes

9.1.8 After-action report that addresses issues identified during contingency/disaster recovery exercises (FCD1, NIST SP 800-34).

Yes

9.1.9 Systems that have alternate processing sites (FCD1, NIST SP 800-34, NIST SP 800-53).

Yes

Section 9: Contingency Planning

9.1.10 **Alternate processing sites are not subject to the same risks as primary sites (FCD1, NIST SP 800-34, NIST SP 800-53).**

Yes

9.1.11 **Backups of information that are performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53).**

Yes

9.1.12 **Contingency planning that considers supply chain threats.**

Yes

9.2 **Please provide any additional information on the effectiveness of the organization's Contingency Planning Program that was not noted in the questions above.**

See OIG evaluation report for additional information.

Section 10: Contractor Systems

10.1 **Has the organization established a program to oversee systems operated on its behalf by contractors or other entities, including organization systems and services residing in the cloud external to the organization? Besides the improvement opportunities that may have been identified by the OIG, does the program includes the following attributes?**

Yes

10.1.1 **Documented policies and procedures for information security oversight of systems operated on the organization's behalf by contractors or other entities, including organization systems and services residing in a public cloud.**

Yes

10.1.2 **The organization obtains sufficient assurance that security controls of such systems and services are effectively implemented and comply with Federal and organization guidelines (NIST SP 800-53: CA-2).**

Yes

Comments:	FCA performed due diligence reviews and monitored security controls for the outsourced financial and payroll systems, but needs to improve oversight of the outsourced electronic official personnel folder (eOPF) system.

10.1.3 **A complete inventory of systems operated on the organization's behalf by contractors or other entities, including organization systems and services residing in a public cloud.**

Yes

Section 10: Contractor Systems

10.1.4 The inventory identifies interfaces between these systems and organization-operated systems (NIST SP 800-53: PM-5).

Yes

10.1.5 The organization requires appropriate agreements (e.g., MOUs, Interconnection Security Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates.

Yes

10.1.6 The inventory of contractor systems is updated at least annually.

Yes

10.1.7 Systems that are owned or operated by contractors or entities, including organization systems and services residing in a public cloud, are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines.

Yes

10.2 Please provide any additional information on the effectiveness of the organization's Contractor Systems Program that was not noted in the questions above.

See OIG evaluation report for additional information.

Section 11: Security Capital Planning

11.1 Has the organization established a security capital planning and investment program for information security? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

Yes

11.1.1 Documented policies and procedures to address information security in the capital planning and investment control (CPIC) process.

Yes

11.1.2 Includes information security requirements as part of the capital planning and investment process.

Yes

11.1.3 Establishes a discrete line item for information security in organizational programming and documentation (NIST SP 800-53: SA-2).

Yes

11.1.4 Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required (NIST SP 800-53: PM-3).

Yes

Section 11: Security Capital Planning

11.1.5 Ensures that information security resources are available for expenditure as planned.

Yes

11.2 Please provide any additional information on the effectiveness of the organization's Security Capital Planning Program that was not noted in the questions above.

See OIG evaluation report for additional information.