USDA
United States Department of Agriculture

U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2018 Federal Information Security Modernization Act

Audit Report 50501-0018-12

October 2018

OFFICE OF INSPECTOR GENERAL

IMPORTANT NOTICE

This audit report contains sensitive information that has been redacted for public release, due to privacy concerns.

U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2018 Federal Information Security Modernization Act (FISMA)

Audit Report 50501-0018-12

As required by FISMA, OIG reviewed USDA's ongoing efforts to improve its information technology security program and practices during fiscal year 2018.

OBJECTIVE

The objectives of this audit were to evaluate the status of USDA's overall IT security program by evaluating the five Cybersecurity Framework security functions: identify, protect, detect, respond, and recover. We also followed up on prior audit recommendations.

REVIEWED

The scope was Department-wide, and we reviewed agency IT audit work completed during FY 2018. This audit covered four agencies and offices operating 117 of the Department's 327 operational systems.

RECOMMENDS

The Department should continue its progress by issuing critical policy and completing actions on the 20 outstanding recommendations from the FYs 2009–2017 FISMA reviews. The Department should establish plans of actions for the 8 new recommendations issued in FY 2018.

WHAT OIG FOUND

The U.S. Department of Agriculture (USDA) continues to take positive steps to improve its information technology (IT) security posture, but many longstanding weaknesses remain. In fiscal years (FY) 2009–2017, the Office of Inspector General (OIG) made 67 recommendations for improving the overall security of USDA's systems—47 recommendations are completed and 20 open recommendations are overdue, an improvement over the 27 open recommendations in FY 2017. Our testing shows weaknesses still exist in 6 of the closed recommendations. We have also issued 8 new recommendations based on security weaknesses identified in FY 2018.

The Office of Management and Budget (OMB) establishes standards for an effective level of security considers "Managed and Measurable" as a sufficient level. However, we found the Department's maturity level to be at the "Defined" level. Based on OMB's criteria, the Department's overall score indicates an ineffective level. The Department and its agencies must also develop and implement an effective plan to mitigate security weaknesses identified in the prior fiscal year recommendations.

Due to existing security weaknesses identified, we continue to report a material weakness in USDA's IT security that should be included in the Department's Federal Managers Financial Integrity Act report. The Department generally agreed with our findings and stated it has developed corrective actions and project plans to address prior year recommendations.

United States Department of Agriculture
Office of Inspector General
Washington, D.C. 20250

DATE: October 12, 2018

AUDIT NUMBER: 50501-0018-12

TO: Gary Washington
Acting Chief Information Officer
Office of Chief Information Officer

ATTN: Megen Davis
Audit Liaison

FROM: Gil H. Harden
Assistant Inspector General for Audit

SUBJECT: U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2018 Federal Information Security Modernization Act

This report presents the results of our audit of the U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2018 Federal Information Security Modernization Act (FISMA). The instructions for fiscal year (FY) 2018 FISMA reporting are outlined in the *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics* (IG FISMA Metrics), V1.0.1, dated May 2018. This report contains our responses to the questions contained in these instructions. Your written response is included, in its entirety, as an attachment to the report. Corrective action plans for the recommendations contained in the report should be provided to OIG within 60 days of this report date.

We appreciate the courtesies and cooperation extended to us by members of your staff during our audits. Portions of this report contains publicly available information and those sections will be posted to our website http://www.usda.gov/oig in the near future. A secured copy of the report in its entirety is being sent to the Director of the Office of Management and Budget.

RMA Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

The United States Department of Agriculture
Federal Information Security Modernization Act of 2014
Audit Report for Fiscal Year 2018

RMA Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

September 27, 2018

The Honorable Phyllis K. Fong
Inspector General, United States Department of Agriculture
1400 Independence Avenue SW
Washington, DC 20250

Re: The U.S. Department of Agriculture, Federal Information Security Modernization Act of 2014 Audit Report for Fiscal Year 2018

Dear Ms. Fong:

RMA Associates, LLC is pleased to submit the U.S. Department of Agriculture (USDA) Federal Information Security Modernization Act of 2014 Audit Report for Fiscal Year (FY) 2018. We conducted the examination in accordance with the *Government Auditing Standards*, issued by the Comptroller General of the United States, and relevant information security standards established by the OMB, DHS, and NIST. We have also prepared the *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.0.1* (May 24, 2018), as shown in Appendix A. These metrics provide reporting requirements across the functional areas to be addressed in the independent assessment of agencies' information security programs. The objective of this audit was to evaluate the effectiveness of the Department's information security program and practices for FY 2018.

We very much appreciate the opportunity to serve you and will be pleased to discuss any questions you may have.

Sincerely,

RMA Associates

RMA Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

The United States Department of Agriculture
Federal Information Security Modernization Act of 2014
Audit Report for Fiscal Year 2018

Table of Contents

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Background

The U.S. Department of Agriculture (USDA) relies extensively on information technology (IT) resources to accomplish its mission. The IT systems and resources strengthen management and oversight of the Department's procurement, property, and finances to ensure resources are utilized as effectively and efficiently as possible. Improving the overall management and security of IT resources and stakeholder information must be a top priority for the Department. While technology enables and enhances the ability to share information instantaneously among stakeholders through computers and networks, it also makes an organization's networks and IT resources vulnerable to malicious activity and exploitation by internal and external sources. Insiders with malicious intent, recreational and institutional hackers, and attacks by foreign intelligence organizations are significant threats to the Department's critical systems.

Federal Information Security Modernization Act of 2014

On December 17, 2002, the President signed the *E-Government Act of 2002* (Public Law 107-347), which includes Title III, entitled the *Federal Information Security Management Act of 2002* (FISMA 2002). Title III requires each Federal agency to develop, document, and implement an agency-wide program to provide information security for the information and systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other sources.

On December 18, 2014, the President signed the *Federal Information Security Modernization Act of 2014* (FISMA), which amended the *Federal Information Security Management Act of 2002* and provided several modifications that modernize Federal security practices to address evolving security concerns. These changes result in less overall reporting, strengthens the use of continuous monitoring in systems, increased focus on the agencies for compliance, and reporting that is more focused on the issues caused by security incidents.

FISMA requires that Federal agencies have an annual independent assessment performed of their information security program and practices to determine the effectiveness of such program and practices, and to report the results of the assessments to the Office of Management and Budget (OMB). In addition to the annual review and reporting requirements, FISMA included new provisions that further strengthened the Federal Government's data and information systems security, such as requiring the development of minimum control standards for agencies' systems. FISMA provided OMB oversight authority of agency security policies and practices and provided authority for the implementation of agency policies and practices for information systems to the Department of Homeland Security (DHS).[1]

[1] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

According to FISMA, the Secretary of DHS must:

> develop and oversee implementation of operational directives requiring agencies to implement OMB standards and guidelines for safeguarding Federal information and systems from a known or reasonably suspected information security threat, vulnerability, or risk. It authorizes the Director of OMB to revise or repeal operational directives that are not in accordance with the Director's policies.[2]

FISMA also "directs the Secretary to consult with, and consider guidance developed by, the National Institute of Standards and Technology (NIST) to ensure that operational directives do not conflict with NIST information security standards."[3]

FISMA directed that agencies:

> submit an annual report regarding major incidents to OMB, DHS, Congress, and the Comptroller General of the Government Accountability Office (GAO). Reports are required to include: (1) threats and threat factors, vulnerabilities, and impacts; (2) risk assessments of affected systems before, and the status of compliance of the systems at the time of, major incidents; (3) detection, response, and remediation actions; (4) the total number of incidents; and (5) a description of the number of individuals affected by, and the information exposed by, major incidents involving a breach of personally identifiable information.[4]

Further, it "requires OMB to ensure the development of guidance for evaluating the effectiveness of information security programs and practices."[5] As part of NIST's statutory role in providing technical guidance to Federal agencies, NIST works with agencies in developing information security standards and guidelines. NIST developed an integrated Risk Management Framework that effectively brings together all the FISMA-related security standards and guidance to promote the development of comprehensive and balanced information security programs by agencies.

[2] Ibid.
[3] Ibid.
[4] Ibid.
[5] Ibid.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

FISMA requires the head of each agency be responsible for:

- Providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency and information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;
- Complying with the requirements of NIST's related policies, procedures, and standards;
- Ensuring information security management processes are integrated with agency strategic, operational, and budgetary planning processes; and
- Ensuring senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including assessing risk, determining the levels of information security, implementing policies to cost-effectively reduce risks, and periodically testing and evaluating security controls.

FISMA requires the Inspector General (IG) to conduct an annual independent assessment to determine the effectiveness of the information security program and practices of its respective agency. These assessments (a) test the effectiveness of information security policies, procedures, and practices of a subset of agency information systems, and (b) assess the effectiveness of an agency's information security policies, procedures, and practices.[6]

FISMA Reporting Metrics

The fiscal year (FY) 2018 IG FISMA reporting metrics[7] were developed as a collaborative effort among OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency (CIGIE), in consultation with the Federal Chief Information Officer (CIO) Council. The FY 2018 metrics represent a continuation of work begun in FY 2016, when the IG metrics[8] were aligned with the five function areas in the *NIST Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework): Identify, Protect, Detect, Respond, and Recover. The Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise and provides IGs with guidance for assessing the maturity of controls to address those risks.

The FY 2018 metrics also mark a continuation of the work that OMB, DHS, and CIGIE undertook in FY 2017 to transition the IG assessments to a maturity model approach. In

[6] NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013).
[7] FY 2018 IG FISMA Reporting Metrics V1.0.1 (May 2018).
[8] FY 2016 IG FISMA Reporting Metrics V1.1.3 (September 2016).

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

previous years, CIGIE, in partnership with OMB and DHS, fully transitioned two of the NIST Cybersecurity Framework function areas, Detect and Respond, to maturity models, with other function areas utilizing maturity model indicators. The FY 2017 IG FISMA Reporting Metrics completed this work by not only transitioning the Identify, Protect, and Recover functions to full maturity models, but also by reorganizing the models themselves to be more intuitive. This alignment with the Cybersecurity Framework helps promote consistent and comparable metrics and criteria in the CIO and IG metrics processes while providing agencies with a meaningful independent assessment of the effectiveness of their information security programs.

Within the maturity model context, agencies should perform a risk assessment and identify the optimal maturity level that achieves cost-effective security based on their missions and risks. IGs assess each of these function levels against the listed criteria when assigning the agency's performance metric rating.

An agency can be assessed at the following five levels in the maturity model:

Table 1

Maturity Level	Maturity Level Description
Level 1: Ad Hoc	Policies, procedures, and strategies were not formalized; activities were performed in an ad hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategies were formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategies were consistently implemented, but quantitative and qualitative effectiveness measures were lacking.
Level 4: Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies were collected across the organization and used to assess them and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategies were fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

The FY 2018 IG FISMA Reporting Metrics state that the "Managed and Measurable" level represents an effective information security program.

DHS' CyberScope website captures agencies' consolidated reporting results. Each Cybersecurity Framework security function area allots points to agencies based on their

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

achievement of various levels of maturity. Ratings throughout the eight domains will be by a simple majority, where the most frequent level across the questions will serve as the domain's rating. For example, if seven questions are in a domain, and the Department receives "Defined" ratings for three questions and "Managed and Measurable" ratings for four questions, then the area rating is "Managed and Measurable." OMB and DHS ensure area ratings are automatically scored when entered into CyberScope, and these scores rate the agency at the higher-level instance when two or more levels are the most frequently rated.

Objectives

The objectives of this audit were to evaluate the status of the Department's overall IT security program and practices by evaluating the five Cybersecurity Framework security functions as divided among eight domains:

- **Identify**, which includes questions pertaining to risk management;
- **Protect**, which includes questions pertaining to configuration management, identity and access management, data protection and privacy, and security training;
- **Detect**, which includes questions pertaining to information security continuous monitoring;
- **Respond**, which includes questions pertaining to incident response; and
- **Recover**, which includes questions pertaining to contingency planning.

The answers to the 67 FISMA Reporting Metrics in Appendix A reflect the results of our testing of the Department's information security program and practices.

This audit also had an objective to review corrective actions taken by the Office of the Chief Information Officer (OCIO) to implement OIG's prior audit recommendations.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2018 Federal Information Security Modernization Act

Findings and Recommendations

This report constitutes our independent audit of the Department's IT security program and practices required by FISMA, based on the FY 2018 IG FISMA Reporting Metrics that use the maturity model indicators. IGs are required to assess the effectiveness of information security programs on a maturity model spectrum in which the foundation levels ensure agencies develop sound policies and procedures and the advanced levels capture the extent to which agencies institutionalize those policies and procedures. This audit reflects the Department's information security program's status based on the completion of 2018 FISMA testing.

USDA is a large, complex organization that includes 36 separate agencies and offices as of the beginning of the audit period, most with their own IT infrastructure. As part of USDA' FY 2018–2022 Strategic Plan, USDA has placed heavy emphasis on the modernization and consolidation of IT infrastructure and services, which includes consolidation of agencies and reduction in the number of CIOs (reducing from 22 to 1, with 9 Assistant CIOs). Regardless of number, each of USDA's agencies, offices, and CIOs, including OCIO, needs to be held accountable for implementing the Department's policies and procedures. Currently, FISMA scores are directly impacted by the agencies selected for detailed testing and the state of selected agencies' information security environment. Therefore, an agency that operates at a lower maturity level will cause USDA's overall maturity level to drop for any given FISMA question. Once compliance by all agencies is attained, FISMA testing results should be consistent, regardless of which agency is selected. This should also improve USDA's overall security posture.

OCIO continues to take positive steps for improving the Department's security posture. For instance, for the Continuous Diagnostic and Mitigation (CDM) project, the Department should expand its continuous diagnostic capabilities by increasing network sensor capacity, automating sensor collections, prioritizing risk alerts, and increasing the coordination with agencies by sharing and reconciling IT technical information. This is a positive step to attain a higher security capability. OMB considers Level 4 "Managed and Measurable" to be an effective level of security.[9] However, we found the Department's maturity level for the eight domains that compose the five function areas to be at Level 2, "Defined." Based on these criteria, the

[9] Per FY 2018 IG FISMA Reporting Metrics V1.0.1 (May 2018), *NIST Special Publication (SP) 800-53, Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations*, defines security control effectiveness as 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 information system in its operational environment or enforcing/mediating established security policies.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Department's overall score indicates an ineffective cybersecurity program. The Department needs to implement its controls and determine they are operating as intended and are producing the desired outcome.

The Department's senior management needs to continue its efforts to make sure that each agency and office understands how its implementation of IT security directly influences the Department's overall security posture and FISMA score. For USDA to attain a secure and sustainable security posture, all agencies and offices must consistently implement Departmental policies based on a standard methodology. When every agency and office complies with USDA's policies, USDA, as a whole, will be FISMA compliant and, more importantly, will have a sustainable security posture.

There are eight new recommendations to address security weaknesses noted this year. If corrective actions are effectively taken at the agency and Departmental levels, security weaknesses within the Department should be mitigated. The Department and its agencies must continue to work in cooperation to develop and implement an effective plan with objectives to mitigate security weaknesses identified in the prior fiscal year recommendations. The plan should prioritize tasks, define goals, and establish realistic timeframes that allow the Department to define and accomplish one or two critical objectives prior to proceeding on to the next set of priorities.

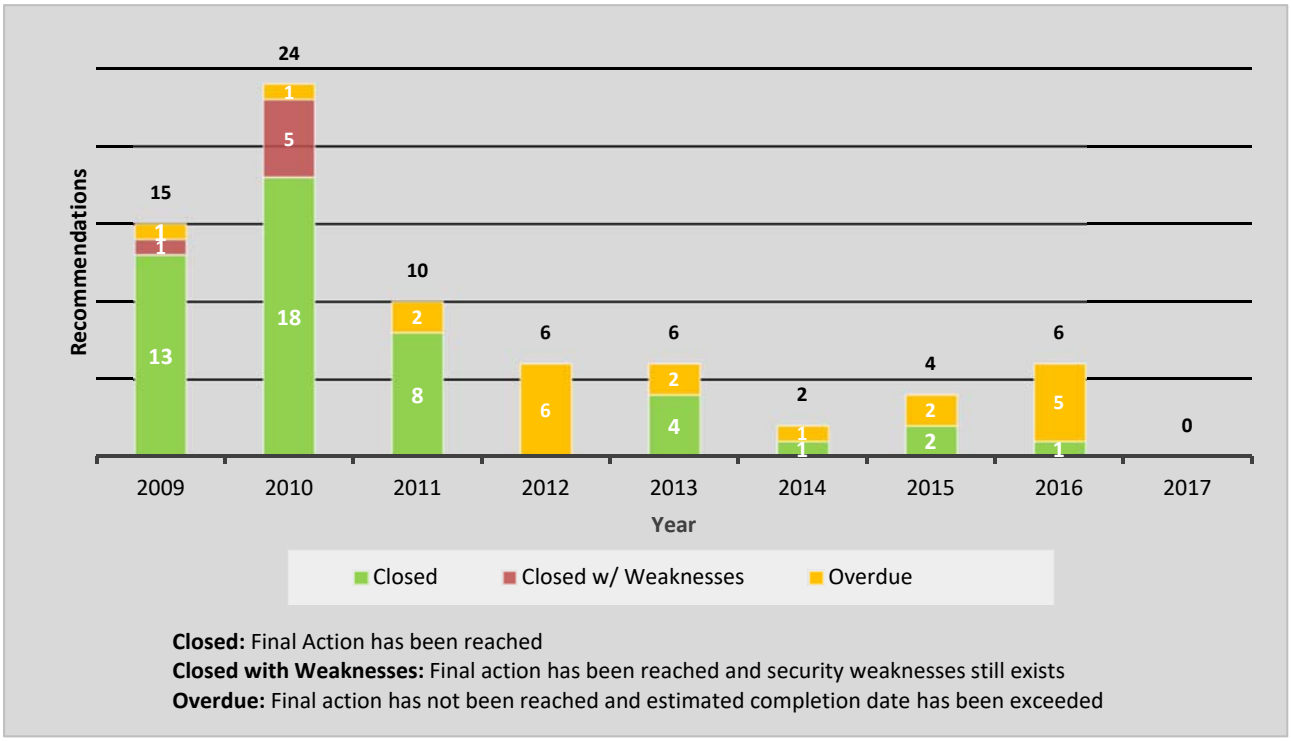
USDA is working to improve IT security, but many longstanding weaknesses remain. We continue to find the Department has not implemented corrective actions in response to prior OIG recommendations. For FISMA audits from 2009 through 2017,[10] OIG made 67 recommendations for improving the overall security of USDA's systems. 47 of the 67 recommendations have been closed, while the 20 open recommendations are overdue.

Our testing this year identified security weaknesses still exist for 6[11] of the 47 closed recommendations. Open recommendations address weaknesses identified in 2[12] of the 6 closed recommendations. New recommendations were issued for the remaining 4 closed recommendations. OCIO generally agreed with our findings and recommendations.

[10] There were no new recommendations made in 2017.
[11] Closed Recommendation 13 from FISMA FY 2009; 3, 10, 17, 18, and 19 from FISMA FY 2010,
[12] Closed Recommendation 13 from FISMA FY 2009 and 10 from FISMA FY 2010

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

FY 2009 through FY 2017 FISMA Recommendations Timeline



Closed: Final Action has been reached
Closed with Weaknesses: Final action has been reached and security weaknesses still exists
Overdue: Final action has not been reached and estimated completion date has been exceeded

Due to existing security weaknesses identified, we are reporting a material weakness in USDA's IT security that should be included in USDA's Federal Managers Financial Integrity Act (FMFIA) report.

In many IT FISMA domain areas, the Department issues policies and procedures and delegates the responsibilities of compliance to the agencies. In spite of the implementation of departmental scorecards and the Cyber Security Assessment Management System (CSAM), centralized oversight needs to be improved. We found due to the decentralization of IT functions in the agencies, the Department does not have an organization-wide view of the many IT processes. We encourage the Department to continue to consolidate common IT functions into a central corporate model and improve the oversight of the agencies' compliance with Department policies.

Exhibit A contains our responses to the OMB/DHS/CIGIE FY 2018 FISMA security questions. These questions were defined on the DHS CyberScope FISMA reporting website. The following paragraphs summarize the key matters discussed in Exhibit A of this report.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Risk Management (Identify)

The Department established a risk management program that operated at the Defined maturity level. In accordance with NIST and OMB guidance,[13] the Department issued a guide that addressed the six-step Risk Management Framework (RMF) process.[14] The RMF Guide provided a basic understanding of the process steps related to the Assessment and Authorization program for IT systems and provides a strong framework for IT risk management. However, the Department did not establish an Enterprise Risk Management (ERM) framework that considered enterprise risk other than IT. Additionally, USDA did not have an appointed Chief Risk Officer (CRO) responsible for managing enterprise risk. The responsibilities of the CRO, as a risk executive function, includes developing and implementing a Department-wide risk management strategy that guides and informs risk decisions, as well as providing oversight for the risk management activities carried out to ensure consistent and effective risk-based decisions.[15]

> **FY 2018 Recommendation 1:** The Department[16] should appoint a CRO executive and develop ERM policies and procedures in accordance with the ERM Playbook: *Enterprise Risk Management for the U.S. Federal Government.*

The Department made significant improvements in the risk management domain by increasing the number of IT systems operating with a valid authorization to operate (ATO). In the prior year FISMA report, 90 of 351 (26 percent)[17] operational systems listed in CSAM[18] were operating with an invalid ATO. Near the end of FY 2018, there were only 16 of 327 (5 percent)[19] operational systems listed in CSAM that were operating with an invalid ATO.

The Department implemented enterprise-wide technologies to inventory and track IT inventory. As such, Departmental-wide listings of IT inventory were maintained, including for IT devices

[13] RMF is a NIST publication that promulgates a common framework intended to improve information security, strengthen risk management, and encourage reciprocity between Federal agencies. NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems* (Feb. 2010), was developed by the Joint Task Force Transformation Initiative Interagency Working Group. Reporting instructions were provided through OMB Memorandum (M)-04-25, *FY 2004 Reporting Instructions for FISMA* (Aug. 23, 2004).
[14] *USDA Six Step RMF Process Guide*, Revision 3.0 (Dec. 2016).
[15] NIST SP 800-39, *Managing Information Security Risk*, Section 2.3.2, *Risk Executive (Function).*
[16] Specifically, the Office of Budget and Program Analysis (OBPA) should be responsible for the implementation of this recommendation.
[17] The number of operational systems and operational systems with expired ATOs was generated from CSAM as of Sept. 11, 2017.
[18] CSAM provides USDA program officials and IT security managers with a web-based secure network capability to assess, document, manage, and report on the status of IT security risk assessments and implementation of Federal and USDA mandated IT security control standards and policies.
[19] The total number of operational systems and operational systems with expired ATOs was generated from CSAM as of August 29, 2018.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

(hardware) and software. However, listings maintained by the agencies sampled did not agree with the Department-wide listings. Effective Department-wide decisions rely on complete and accurate information, which cannot be achieved without established inventory reconciliation policies and procedures to maintain a full population of IT inventory.

> **FY 2018 Recommendation 2:** OCIO should document its plan to continue to implement technologies to improve hardware and software asset management within the USDA IT enterprise. Additionally, OCIO should document its internal processes for hardware and software inventory verification and reconciliation by agencies against the Department's centralized enterprise-wide asset management and systems inventory solutions.

The Department maintained the listing of cloud and third-party (contractor) systems in CSAM. However, agencies sampled were unable to provide a listing of such systems that agreed to the listing in CSAM. The Department closed a prior year recommendation related to the inventory of contractor and non-contractor systems; however, based on current year findings, we believe remediation is still necessary for this recommendation.[20]

> **FY 2018 Recommendation 3:** OCIO should verify and reconcile listings of cloud and third-party (contractor) systems against agency records.

The Department did not have an effective process for remediating known vulnerabilities on IT devices in a timely manner. In some of the agencies sampled, a significant percentage of critical and high vulnerabilities were outstanding for more than 2 years and some over 5 years.[21] For example, in one agency 49 percent of critical and high vulnerabilities were outstanding for 2 to 5 years, while an additional 12 percent were outstanding for more than five years. The Department's policy states critical vulnerabilities must be corrected within 30 days or a Plan of Action and Milestones (POA&M) must be established.[22] POA&Ms were not created for all critical vulnerabilities that were not corrected within 30 days.

> **FY 2018 Recommendation 4:** OCIO should update the Department policy for vulnerability management to specify time constraints for resolving high vulnerabilities.

> **FY 2018 Recommendation 5:** OCIO should develop, document and implement enterprise-wide procedures and processes for vulnerability management to regularly scan and patch vulnerabilities and upgrade software to address security deficiencies identified during the agency scans. This plan should include a reconciliation of scans performed by the Department and the scans performed by the agencies. Additionally, import scanning

[20] Recommendation 19 from FISMA FY 2010.
[21] IT devices were either placed in service with known vulnerabilities or the vulnerabilities were outstanding on the device for an excessive amount of time.
[22] Departmental Manual (DM) 3530-001, *Vulnerability Scan Procedures* (July 2005)

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

results from agencies into the Department's centralized and enterprise-wide vulnerability scanning solution (if technical functionality exists).

Systems and networks supporting mission-focused software were not patched or upgraded in a timely manner. Patching or upgrading is usually the most effective way to mitigate security flaws in software and is often the only fully effective solution. Failure to apply patches or upgrades in a timely manner increases the risk that known vulnerabilities will be exploited. Software no longer supported by vendors was in use and exposed the Department to vulnerabilities that are difficult to effectively mitigate. Use of unsupported software increases the risk that known vulnerabilities will be exploited. No waivers were provided for the unsupported software.

> **FY 2018 Recommendation 6:** OCIO should design and implement a strategic Department-wide plan to address unsupported software which are no longer supported by the vendor.

In addition to the findings noted above, there were four prior OIG audit recommendations[23] outstanding that relate to the risk management domain.

Configuration Management (Protect)

The Department established and maintained a security configuration management program that operated at the Defined maturity level. In accordance with NIST and OMB guidance, the Department established a configuration management Department Regulation (DR)[24] that provided guidance to all agencies and staff for implementing configuration management. The DR established standard baseline configurations for all applicable operating systems; however, the sampled agencies did not have baseline configurations for all network devices or systems. Patch levels and upgrades were not consistently included in baseline configurations. Additionally, high and critical vulnerabilities, which should not be allowed in a secure baseline, were found in agency scanning results.

The Department and two of the agencies sampled established and maintained a configuration management Change Control Board. However, one of the agencies sampled did not have a Change Control/Change Advisory Board.

The Department adopted the Trusted Internet Connection (TIC) program to assist in protecting its network; however, the TIC program does not include security controls for mobile devices.

[23] Overdue Recommendation 14 from FISMA FY 2010; 4 and 5 from FISMA FY 2012; and 1 from FISMA FY 2016.
[24] DR 3520-002, *Configuration Management.*

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

There are three overdue recommendations relating to configuration management.[25]

Identity and Access Management (Protect)

The Department established an identity and access management program that operated at the Consistently Implemented maturity level. The Department developed multiple policies[26] that compose the identity and access management program in compliance with NIST standards. Additionally, the Department adequately planned for the implementation of Personal Identity Verification (PIV) for non-privileged and privileged access in accordance with Government standards.[27] The Department and two of the agencies sampled had high percentages of use of PIV for all users; however, one of the agencies sampled was below the target threshold of adopted PIV usage for non-privileged users. Additionally, there were three separated employees from one sampled agency who did not have their user accounts fully disabled or deactivated.

The Department defined a policy[28] for assigning personnel risk designations; however, one of the agencies sampled did not assign risk designations. Without personnel risk designation levels, the Department did not have an organization-wide view of the personnel risk and cannot ensure the necessary background investigations are performed for personnel with sensitive duties.

Additionally, the Department did not implement an entity-wide single sign-on solution.

There are currently four overdue recommendations relating to identity and access management.[29]

Data Protection and Privacy (Protect)

The Department did not establish a data protection and privacy program that operated at the Defined maturity level. Certain policies were established;[30] however, there were several that were out-of-date and did not reference updated NIST and OMB A-130 requirements. Additionally, there was no finalized, overarching data protection and privacy policy. The lack of

[25] Overdue Recommendation 2 from FISMA FY 2013; 2 from FISMA FY 2012; and 4 from FISMA FY 2011.
[26] DR 3640-001, *Identity, Credential, and Access Management*; DR 3505-003, *Access Control for Information and Information Systems*; DR 4620-002, *Common Identification Standard for U.S. Department of Agriculture*.
[27] The Executive Branch mandate entitled, *Homeland Security Presidential Directive 12* (HSPD-12) (Aug. 2004), requires Federal agencies to develop and deploy for all of their employees and contract personnel a PIV credential that is used as a standardized, interoperable card capable of being used as employee identification and allows for both physical and information technology system access.
[28] DR 3505-003, *Access Control for Information and Information Systems*.
[29] Overdue Recommendation 4 from FISMA FY 2015; 4 from FISMA FY 2013; and 1 and 2 from FISMA FY 2016.
[30] DM 3515-002, *Privacy Impact Assessment* (Feb. 2005); Memo, *Minimum Safeguards for Protecting Personally Identifiable Information (PII)* (Aug. 2016).

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

updated policies and procedures led to a decentralized governance of PII throughout the Department. The sampled agencies had clear practices in place; however, the practices were inconsistently implemented and there was no evidence Department policies were communicated and understood by agency stakeholders.

The Department maintained an inventory of the collection and use of PII through the utilization of reports, such as Privacy Score Cards, Privacy Threshold Analysis, and System Privacy Summary Reports. However, the Department records did not consistently match records kept at the agency.

> **FY 2018 Recommendation 7:** The Department should develop privacy policies and procedures in accordance with NIST and OMB A-130 requirements. In addition, OCIO and the Chief Privacy Officer should conduct a thorough gap analysis of existing USDA policy, procedures and guidance, and publish an updated Privacy Act Compliance Departmental Directive to include current NIST and OMB Privacy Act related guidance and requirements.

Security Training (Protect)

The Department established a security training program that operated at a Defined maturity level. Policies[31] and procedures[32] met all NIST requirements for annual security awareness training. A aemorandum was issued on September 29, 2017, which required all users to complete the FY 2018 Information Security Awareness (ISA) Training by March 30, 2018.[33] Per the memorandum, network access would be removed for all users who did not complete the training by March 30, 2018. As of May 11, 2018, the overall Department completion rate was 93 percent. However, the sampled agencies had completion rates of 61 percent, 82 percent, and 80 percent, respectively, as of that date.[34] Additionally, two of the sampled agencies did not provide evidence that specialized training courses were provided in FY 2018. In 2016, OIG recommended the Department identify all users who need security awareness training, populate the training repository completely with those individuals, and ensure they receive the required training.[35] This overdue recommendation remains open.

[31] DR 3545-001, *Information Security Awareness and Training Policy* (Oct. 2013).
[32] Departmental SOP-CPPO-018, Information Security Awareness Training Standard Operating Procedures (Apr. 2011).
[33] Memo, *Fiscal Year (FY) 2018 Mandatory Information Security Awareness (ISA) Training* (Sept. 2017).
[34] AgLearn ISA Status Report, May 11, 2018
[35] Overdue Recommendation 2 from FISMA FY 2016.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Information Security Continuous Monitoring (ISCM) (Detect)

The Department established an ISCM program that operated at the Defined maturity level. A policy[36] and a strategic plan[37] for ISCM strategy were established. As discussed in the risk management section above, the Department made a significant improvement to information security by increasing the number of operational systems that were operating with a valid ATO. However, the ISCM strategy is composed of multiple programs which have not yet reached the Consistently Implemented maturity level, including risk management, configuration management, incident management, and POA&M management. Additionally, the Department was still in the process of integrating all its ICSM strategy activities, such as incorporating tools from DHS CDM Phase 2 that will automate ICSM related metrics.

Incident Response (Respond)

The Department established an incident response and reporting program that operated at the Defined maturity level. The Department established a new incident management policy, which was signed in late July 2018.[38] The policy establishes the guidelines and facilitates implementation for the Department to respond to and report cybersecurity events. The effective implementation of this policy should allow the Department to operate at a higher maturity level; however, for the FY 2018 reporting period, it cannot be concluded the Department operated at the consistently implemented maturity level given the policy was signed at the end of the audit period. It is too early to determine whether the practice in place is compliant with the new policy. There are currently two overdue recommendations relating to incident response.[39]

Contingency Planning (Recover)

The Department established a contingency planning program that operated at the Defined maturity level. A policy,[40] procedural manual,[41] and standard template[42] were established to implement the enterprise-wide business continuity/disaster recovery program. However, the Department did not implement the necessary oversight, enforcement mechanisms, and controls to ensure all contingency plans were tested and the results of the tests were reviewed to initiate corrective actions (as needed) to strengthen the effectiveness of each contingency plan.

[36] DR 3540-003, *Security Assessment and Authorization* (Aug. 2014)
[37] *USDA Information Security Continuous Monitoring Strategic Plan*, Version 1.9 (Apr. 2017)
[38] DR 3505-005, *Cybersecurity Incident Management*.
[39] Overdue Recommendation 3 from FISMA FY 2012 and 2 from FISMA FY 2014.
[40] DR 3571-001, *Information System Contingency Planning and Disaster Recovery Planning* (June 2016).
[41] *Contingency Plan Exercise Handbook*, Revision 2.1 (June 2017).
[42] *Contingency Plan Template*, v1.5 (June 2017).

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

A total of 82 of 330 (25 percent) operational systems did not have contingency plan testing performed within the past year.[43] Testing of system contingency plans is critical to ensuring effective system contingency plans are in place. Without effective system contingency plans, USDA's mission data is at a higher risk of loss due to an unscheduled disruption. Specifically, unscheduled disruptions in operations may debilitate USDA in such a way that it may be unable to recover and continue operations of all necessary systems and functions in a timely manner. The Department closed a prior year recommendation[44] related to contingency planning; however, based on current year findings, we believe remediation is still necessary for this recommendation.

> **FY 2018 Recommendation 8:** The Department should design and implement the necessary oversight and enforcement mechanisms and controls to ensure all system contingency plans are tested annually and the results of all tests are reviewed annually to ensure corrective actions can be initiated, as necessary.

[43] CSAM report as of August 27, 2018. Additionally, DR 3571-001, *Information System Contingency Planning and Disaster Recover Planning* (June 2016), states that contingency plans shall be tested at least annually.
[44] Closed Recommendation 17 from FISMA FY 2010.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Scope and Methodology

Scope

The scope of our review was Department-wide. In total, our FY 2018 FISMA audit work covered four agencies and offices:

- Agriculture Marketing Service (AMS);
- National Institute of Food and Agriculture (NIFA);
- Natural Resources Conservation Services (NRCS); and
- OCIO.

As of August 29, 2018, these agencies and offices operated 117 of the Department's 327 operational systems.

Methodology

We conducted this audit in accordance with *Government Auditing Standards*. The audit was designed to determine whether the Department implemented selected security controls for selected information systems in support of the *Federal Information Security Modernization Act of 2014*. Our audit was conducted for FY 2018 and consisted of testing the 67 FISMA Reporting Metrics issued by DHS.

We also conducted this audit in accordance with generally accepted government auditing standards (GAGAS). 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The overall strategy of our audit considered *NIST 800-53A, Guide for Assessing Security Controls in Federal Information Systems and Organizations, NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations,* and the FISMA guidance from CIGIE, OMB, and DHS. Our testing procedures were developed from NIST SP 800-53A. We determined the overall maturity level of each of the eight domains by a simple majority of the competent scores of the maturity level of each question within the domain, in accordance with the *FY 2018 IG FISMA Reporting Metrics V1.0.1*.

For testing the operating effectiveness of the security controls, we exercised professional judgment in determining the number of items to select for testing and the method to be used to select items. We considered relative risk and the significance or criticality of the specific items

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

in achieving the related control objectives. We also considered the severity of a deficiency related to the control activity.

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Abbreviations

AC .....access control
AM.....asset management
AMS.....Agriculture Marketing Service
AT.....awareness and training
ATO.....authorization to operate
BCP.....Business Continuity Plan
BE .....business environment
BIA.....Business Impact Analysis
CA.....Security Assessment and Authorization
CCB.....Change Control Board
CDM.....Continuous Diagnostics and Mitigation
CFO.....Chief Financial Officer
CIGIE.....Council of the Inspectors General on Integrity and Efficiency
CIO.....Chief Information Officer
CIS.....Center for Internet Security
CM.....configuration management
CO.....communications
CP.....contingency planning
CSAM.....Cyber Security Assessment Management System
CSF.....Cybersecurity Framework
CSIP……Cybersecurity Strategy and Implementation Plan
DE.....detect
DHS.....Department of Homeland Security
DR……Departmental Regulation
ERM.....Enterprise Risk Management
FAR.....Federal Acquisition Regulation
FCD.....Federal Continuity Directive
FEA.....Federal Enterprise Architecture
FICAM.....Federal Identity, Credential, and Access Management
FIPS.....Federal Information Processing Standards
FISMA.....Federal Information Security Modernization Act of 2014
FY.....fiscal year
GAO.....Government Accountability Office
GISRA.....Government Information Security Reform Act
GV.....governance
HSPD .....Homeland Security Presidential Directive
IA.....identification and authentication
ICAM.....Identity Credential and Access Management

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

ID.....iIdentify
IG.....Inspector General
IP.....Information Protection Processes and Procedures
IR.....incident response
ISCM.....Information Security Continuous Monitoring
IT.....information technology
NARA.....National Archives and Records Administration
NIFA.....National Institute of Food and Agriculture
NRCS.....Natural Resources Conservation Service
NIST.....National Institute of Standards and Technology
OCIO.....Office of Chief Information Officer
OIG.....Office of Inspector General
OMB.....Office of Management and Budget
PIV.....Personal Identity Verification
PL.....planning
PM.....Program Management
POA&M.....Plan of Action and Milestones
PR.....protect
PS.....personnel security
RA.....risk assessment
RC.....recover
RM.....Risk Management Strategy
RMF.....Risk Management Framework
SA.....System and Services Acquisition
SANS.....Sysadmin, Audit, Network, Security
SAT.....Security Awareness Training
SDLC.....System Development Life Cycle
SI.....System and Information Integrity
SIEM.....Security Information and Event Management
SP.....Special Publications
TIC.....Trusted Internet Connections
US-CERT.....United States Computer Emergency Readiness Team
USDA.....Department of Agriculture
USGCB.....United States Government Configuration Baseline

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

Criteria

We focused our FISMA audit approach on Federal information security guidelines developed by DHS, NIST, and OMB. NIST Special Publications (SPs) provide guidelines that were considered essential to the development and implementation of the Department's security programs. The following is a listing of the criteria used in the performance of the FY 2018 FISMA audit:

NIST Federal Information Processing Standards (FIPS) and Special Publications

- FIPS Publication 199, *Standards for Security Categorization of Federal Information, and Information Systems*
- FIPS Publication 200, *Minimum Security Requirements for Federal Information, and Information Systems*
- FIPS Publication 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*
- NIST SP 800-30, *Risk Management Guide for Information Technology Systems*
- NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*
- NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
- NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*
- NIST SP 800-40, *Guide to Enterprise Patch Management Technologies*
- NIST SP 800-50, *Building an Information Technology Security Awareness, and Training Program*
- NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
- NIST SP 800-53A Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*
- NIST SP 800-60, *Guide for Mapping Types of Information, and Information Systems to Security Categories*
- NIST SP 800-61 Revision 1, *Computer Security Incident Handling Guide*
- NIST SP 800-63, *Digital Identity Guidelines*
- NIST SP 800-83, *Guide to Malware Prevention and Handling*
- NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*
- NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*
- NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*
- NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*

1005 N. Glebe Road, Suite 210
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

- NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems, and Organizations*
- NIST SP 800-181, *NICE Cybersecurity Workforce Framework*

OMB Policy Directives

- OMB Memorandum M-18-02, *Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements*
- OMB Memorandum M-17-09, *FY 2017 Management of Federal High-Value Assets*
- OMB Memorandum M-16-04, *FY 2016 Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*
- OMB Memorandum M-14-03, *FY 2014 Enhancing the Security of Federal Information and Information Systems*
- OMB Memorandum M-08-05, *FY 2008 Implementation of Trusted Internet Connections (TIC)*
- OMB Memorandum M-04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*
- OMB Circular A-130, *Managing Information as a Strategic Resource*

Department of Homeland Security

- *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.0.1 May 24, 2018*

The subsequent section of the report “Exhibit A” is not being publicly released due to the sensitive security content.

AGENCY'S
RESPONSE TO AUDIT REPORT

United States Department of Agriculture
Office of the Secretary
Office of Budget and Program Analysis
Washington, D.C. 20250

TO: Gil Harden
Assistant Inspector General for Audit
Office of Inspector General

OCT 05 2018

FROM: Erica Navarro
Director

SUBJECT: The U.S. Department of Agriculture, Fiscal Year 2018 Federal Information Security Modernization Act Draft Audit Report. #50501-0018-12.

The Office of Budget and Program Analysis (OBPA) appreciates the opportunity to review the subject draft audit report. The draft report recommends that the Department appoint a Chief Risk Officer (CRO) executive and develop Enterprise Risk Management (ERM) policies and procedures in accordance with the ERM Playbook: Enterprise Risk Management for the U.S. Federal Government. OBPA concurs with the recommendation to appoint a CRO and will work with Department officials to have an executive assigned those responsibilities. Once the CRO is named, OBPA will work with the CRO to develop and have in place an ERM framework consistent with the principles of ERM by October 2019.

cc: Jane Bannon, OIG, Director IT Audit Operations
Melissa Rumsey, OIG
Megen Davis, OCIO Audit Liaison
Cynthia Schwind, OIS FISMA Coordinator

United States Department of Agriculture

Departmental Administration

Office of the Chief Information Officer

1400 Independence Avenue S.W.
Washington, DC 20250

TO: Gil H. Harden
Assistant Inspector General for Audit
Office of Inspector General

FROM: Gary S. Washington
Chief Information Officer
Office of the Chief Information Officer

SUBJECT: Office of Inspector General Audit 50501-0018-12, United States Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2018 Federal Information Security Management Act.

The Office of the Chief Information Officer (OCIO) appreciates the opportunity to review the subject draft audit report. The OCIO has reviewed the report and agrees with the Office of Inspector General (OIG) assessment of the Department's IT Security Program. OCIO is developing corrective actions and project plans to address the draft audit recommendations, and to document those actions sufficiently to achieve final action by the Office of the Chief Financial Officer (OCFO).

If additional information is needed, please contact Megen Davis, OCIO Audit Liaison at (301) 504-4299 or via email at megen.davis@wdc.usda.gov.

cc: Tacy Summersett, OCIO, Acting Chief Information Security Officer
Johanna Briscoe, DM, Chief of Staff
Lance Moore, OIG, Assistant Regional Inspector General
Jane Bannon, OIG, Director IT Audit Operations
Tonya Judkins, OCIO Chief of Staff
Brad Rounding, Director, OIS Security Operations Division
Doug Parry, Director, OIS Security Integration Division
Christopher Wren, OCIO Audit Liaison
Megen Davis, OCIO Audit Liaison
Jane Davis, OCIO Office Manager
Cynthia Schwind, OIS FISMA Coordinator

Learn more about USDA OIG
Visit our website: www.usda.gov/oig/index.htm
Follow us on Twitter: @OIGUSDA

How to Report Suspected Wrongdoing in USDA Programs

Fraud, Waste, and Abuse
File complaint online: www.usda.gov/oig/hotline.htm

Monday–Friday, 9:00 a.m.– 3:00 p.m. ET
In Washington, DC 202-690-1622
Outside DC 800-424-9121
TDD (Call Collect) 202-690-1202

Bribes or Gratuities
202-720-7257 (24 hours)