USDA
United States Department of Agriculture

U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2019 Federal Information Security Modernization Act

Audit 50503-0002-12

October 2019

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 2019 Federal Information Security Modernization Act (FISMA)

Audit Report 50503-0002-12

As required by FISMA, OIG reviewed USDA's ongoing efforts to improve its information technology security program and practices during fiscal year 2019.

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 reviewed corrective actions taken by the Office of the Chief Information Officer (OCIO) to implement OIG's prior audit recommendations.

REVIEWED

The scope was Departmentwide, and we reviewed agency IT audit work completed during FY 2019. This audit covered four agencies and offices operating 75 of the Department's 328 operational systems.

RECOMMENDS

We recommend that the Department review and identify the full population and last review date of all IT policies and procedures, revise them as needed, and disseminate them to employees; create a monitoring plan to ensure that all policies and procedures are reviewed and updated; and remove unauthorized software from USDA systems.

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) 2009–2018, the Office of Inspector General (OIG) made 75 recommendations for improving the overall security of USDA's systems—71 recommendations are completed and 4 recommendations are scheduled for closure after the date of our report. We have also issued 3 new recommendations based on security weaknesses identified in FY 2019. One recommendation reopens a previously closed recommendation because the implemented remediation was ineffective.

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. In our detailed testing of the 67 FISMA Reporting Metrics, we found the Department increased its maturity level for 22 metrics. One metric's maturity level was downgraded because of a new requirement related to supply chain risk management, and the maturity level did not change for 44 metrics. 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.

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

DATE: October 30, 2019

AUDIT NUMBER: 50503-0002-12

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

ATTN: Megen Davis
Audit Liaison

FROM: Gil H. Harden Gil H. Harden
Assistant Inspector General for Audit

SUBJECT: U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2019 Federal Information Security Modernization Act

This report presents the results of the U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2019 Federal Information Security Modernization Act (FISMA) audit. The instructions for fiscal year (FY) 2019 FISMA reporting are outlined in the *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics* (IG FISMA Metrics), v1.3, dated April 9, 2019. This report contains our responses to the questions contained in these instructions. Your written response is included in its entirety at the end of the report. Corrective action plans for the recommendations contained in the report should be provided to the Office of Inspector General (OIG) within 60 days of this report date.

We appreciate the courtesies and cooperation extended to us by members of your staff during audit fieldwork and subsequent discussions. Portions of this report contain 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 610
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 2019

RMA | Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone : (571) 429-6600
www.rmafed.com

September 24, 2019

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 2019

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) 2019. We conducted the audit in accordance with the *Government Auditing Standards*, issued by the Comptroller General of the United States, and relevant information security standards established by the Office of Management and Budget (OMB), the Department of Homeland Security (DHS), and the National Institute of Standards and Technology (NIST). We have also prepared the *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.3* (April 9, 2019), 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 2019.

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

Sincerely,

RMA Associates

The United States Department of Agriculture
Federal Information Security Modernization Act of 2014
Audit Report for Fiscal Year 2019

Table of Contents

Background

The United States 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 among stakeholders instantaneously 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 foreign intelligence organizations' attacks are significant threats to the Department's critical systems.

KEY CHANGES TO THE FY 2019 IG FISMA METRICS

One of the goals of the annual Federal Information Security Modernization Act of 2014 (FISMA) audit is to assess the agency's progress toward achieving outcomes that strengthen Federal cybersecurity, including implementing the Administration's priorities and best practices. The *FY 2019 CIO FISMA Metrics*, OMB Memorandum M-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*, and the Department of Homeland Security's (DHS) Binding Operational Directive 18-02, *Securing High Value Assets*, have placed additional emphasis on the enhancement of the High Value Asset (HVA) program. As such, the *Fiscal Year (FY) 2019 Inspector General (IG) FISMA Reporting Metrics* include additional maturity indicators and criteria references regarding the evaluation of the effectiveness of agencies' HVA programs.

Furthermore, on December 21, 2018, the Strengthening and Enhancing Cyber-Capabilities by Utilizing Risk Exposure Technology Act of 2018 (SECURE Technology Act) established new requirements for supply chain risk management. The *FY 2019 IG FISMA Reporting Metrics* were updated to gauge agencies' preparedness in addressing these new requirements.

Since the publication of the *FY 2018 IG FISMA Reporting Metrics*, the National Institute of Standards and Technology (NIST) has updated several of its Special Publications to enhance existing criteria, such as NIST SP 800-37 Revision 2 and NIST SP 800-160 (Volume 1). These updates include changes to criteria that impact the IG FISMA metrics, such as an alignment with the constructs in the NIST Cybersecurity Framework, the integration of privacy risk management processes, alignment with system life cycle security engineering processes, and the incorporation of supply chain risk management processes. While the updates will not go into full effect until 1 year after their respective publications, the criteria references in the *FY 2019 IG FISMA Reporting Metrics* were updated to reflect these changes.

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 agencywide 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 amends FISMA 2002 and provides several modifications that modernize Federal security practices to address evolving security concerns. These changes reduce overall reporting, strengthen the use of continuous monitoring in systems, increase focus on the agencies for compliance, and produce reporting more focused on issues caused by security incidents.

FISMA requires Federal agencies to have an annual independent assessment performed of their information security program and practices to determine the effectiveness of such program and practices and report the results of the assessments to the Office of Management and Budget (OMB). In addition to the annual review and reporting requirements, FISMA includes 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 provides OMB oversight authority of agency security policies and practices and provides authority for the implementation of agency policies and practices for information systems to the Department of Homeland Security (DHS).[1]

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 "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]

Additionally, FISMA directs Federal agencies to:

> 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

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

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, FISMA "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 also develops 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 for all Federal agencies.

FISMA requires the head of each agency to 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, 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 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 *FY 2019 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 2019 metrics

[4] Ibid.
[5] Ibid.
[6] NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (Apr. 2013).
[7] *FY 2019 IG FISMA Reporting Metrics v1.3* (Apr. 2019).

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 2019 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 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 reorganizing the models 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. Also, this year, Protect function metrics were added to address the new requirements for HVA and supply chain management.

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: IG Evaluation Maturity Levels

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.

[8] *FY 2016 IG FISMA Reporting Metrics v1.1.3* (Sep. 2016).

Maturity Level	Maturity Level Description
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 2019 IG FISMA Reporting Metrics* state 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 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.

U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2019 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 2019 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 2019 FISMA testing.

USDA is a large, complex organization and includes 36 separate agencies and offices as of the beginning of the audit period, most with their own IT infrastructure. As part of USDA's 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 (reduced from 22 to 1, with 9 Assistant CIOs). Regardless of the 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 consistency should also improve USDA's overall security posture.

One of the strategic goals is to deliver USDA programs that ensure the Department's programs are delivered efficiently, effectively, and with integrity and a focus on customer service. The Department continues to modernize and consolidate IT infrastructure and services. The Department publishes biweekly dashboards to provide information to its stakeholders that measure progress toward the Departmental security goals. The Department is focused on improving the efficiency and effectiveness of its management activities across the Department and is centralizing business functions in each Mission Area to help ensure better alignment.

OCIO started several initiatives in FY 2019:

- The Department made significant improvements in the incident response domain by publishing official policies and procedures to govern the processes in place.
- OCIO made progress implementing recommendations that addressed many longstanding weaknesses.
- OCIO began revising its Departmental Manuals (DMs) and Departmental Regulations (DRs) to be in compliance with NIST 800-53 Revision 4 controls. However, most of the revisions were issued at the end of our fieldwork. These revised DMs and DRs will take time to implement and to show effectiveness in operations.

- OCIO continues to modernize the eAuthentication shared service (eAuth) and focus on further expanding the enforcement of Personal Identity Verification (PIV) credentials for logical access.
- OCIO continues to foster a strategic approach to data management and pursuing data-driven capabilities that result in executive dashboard solutions of USDA-wide data.

Although the Department has demonstrated a concerted effort to close many of the outstanding recommendations in FY 2019, significant security weaknesses still exist. During the current year, the Department completed corrective actions by revising its policies and procedures to be compliant with current Federal requirements. However, these policies and procedures take time to become effective. The Department must inform employees and contractors of the revised policies and procedures, and those employees and contractors must perform the control activities consistently throughout the Department to be effective. In addition, some prior recommendations remain open, and our current year testing found additional security weaknesses.

The Department's overall maturity level remains at Level 2, "Defined." At Level 2, policies, procedures, and strategies are formalized and documented, but they are not consistently implemented. DHS considers information security programs operating at an effective level of security at Level 4, "Managed and Measurable." At Level 4, policies, procedures, and strategies are effective throughout the organization, and quantitative and qualitative factors assess the effectiveness of policies, procedures, and strategies. Also, the organization revises its policies, procedures, and strategies as a result of their assessments. Due to the Department's maturity of "Defined," we are reporting a material weakness in the Department's IT security program. The Department should report this weakness in its Federal Managers' Financial Integrity Act (FMFIA) report.

In our detailed testing of the 67 FISMA Reporting Metrics, we found the Department increased its maturity level for 22 metrics. One metric's maturity level was downgraded because of a new requirement related to supply chain risk management, and the maturity level did not change for 44 metrics.

The 67 FISMA Reporting Metrics are grouped into 8 domains. For one of those domains, Incident Response, the Department increased its maturity level from Level 1, "Ad Hoc" to Level 4, "Managed and Measurable," while the remaining seven domains were at Level 2, "Defined."

The Department's senior management needs to continue its efforts to centralize and manage common functions at the Departmental level. It is more efficient and effective to control, monitor, evaluate, and react to centrally managed controls than allow individual agencies to manage these control activities.

USDA worked extensively in FY 2019 to improve IT security through the closure of longstanding weaknesses. The Department reduced the number of outstanding OIG prior year recommendations through the implementation of corrective actions. For FISMA audits 2009 through 2018, OIG issued 75 recommendations for improving the overall security of USDA's systems. The

Department's corrective actions closed 71 recommendations, while 4 recommendations are scheduled for closure after the date of our report.

For FY 2019 we are making three recommendations. One of those recommendations reopens a closed recommendation because the implemented remediation was ineffective. We acknowledge that OCIO made a concerted effort to close many of the outstanding recommendations. OCIO generally agreed with our findings and recommendations.

In many IT FISMA domain areas, the Department issues policies and procedures and delegates the responsibilities of compliance to the agencies. Despite the implementation of Departmental scorecards and the Cyber Security Assessment Management System (CSAM), more centralized oversight is needed. Due to the decentralization of IT functions in the agencies, the Department does not have an organization-wide view of the many IT processes and controls. 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 Departmental policies.

Appendix A contains our responses to the OMB/DHS/CIGIE FY 2019 FISMA security questions. These questions are defined on the DHS CyberScope FISMA reporting website. The following paragraphs summarize the key matters discussed in Appendix A of this report.

Risk Management (Identify)

Our testing noted outdated policies and procedures, non-mission software, and outstanding recommendations. As a result, the Department established and maintained a security Risk Management program that operated at the "Defined" maturity level.[9]

Policies are the principal method through which USDA communicates its mission, strategic plan, goals, and objectives. Policy is the fundamental defense in safeguarding assets and defines operational expectations. USDA is responsible for designing the policies and procedures to fit its circumstances and building them as an integral part of the entity's operations.

During our review of USDA's IT policies and procedures, we found that there were 18 DMs and 13 DRs in the Cyber Security series (series beginning with 3500).[10] Only 1 of the 18 DMs has evidence of review within the last 3 years, while 9 of the 13 DRs have evidence of review within the last 5 years. Although USDA does have security practices in place, there were instances in which current policies or procedures were not in place to support operations. With outdated policies and procedures, there is an increased risk that security practices are unclear, misunderstood, and improperly implemented and do not keep USDA safe.

NIST Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, has 18 controls specifically addressing policies and procedures. The first control of each family specifies that the organization must review and update the current policies and procedures within an organization-defined frequency.

USDA is a significant organization in size and scope, with a complex IT infrastructure. The Department's process for updating policies and procedures involves many layers of review and may, at times, require the review of multiple authorities and divisions. As such, the process to review, modify, approve, and distribute policies and procedures can take a significant amount of time and may not keep pace with the rapidly-changing IT security environment.

- **FY 2019 Recommendation 1:** Perform a complete review to identify the full population and last review date of all IT policies and procedures maintained by the Department. For each policy/procedure that does not have evidence of review within the time frame prescribed by DR 0100-001, perform a review and make appropriate revisions before obtaining the appropriate approver's signature and timestamp. Revised policies/procedures should be disseminated to employees as required by NIST SP 800-53 Revision 4.

- **FY 2019 Recommendation 2:** Create a monitoring plan to ensure that all policies and

[9] CyberScope calculates the maturity level of each domain by determining a simple majority of each answer within the domain; it does not account for the impact of the higher maturity level within a domain. CyberScope calculated the maturity level of Risk Management as Level 1, "Ad Hoc." By our testing, we felt that the calculated maturity level did not accurately reflect the maturity level of the domain. As such, we assessed the maturity level of Risk Management as Level 2, "Defined."

[10] Data as of June 12, 2019, https://www.ocio.usda.gov/policy-directives-records-forms/directives-categories.

procedures are reviewed and updated in accordance with the timeliness requirements established in DR 0100-001.

We found instances of personal use software on the USDA's network that were not supported by evidence of approved personal use software request forms, which would demonstrate a review of software for appropriate use. Examples included over 200 instances of computer gaming software as well as 56 copies of income tax preparation software for years 1998 to 2015. An additional concern was that the tax preparation software may contain Personally Identifiable Information (PII). We did not find any evidence that the Department monitored personal use software to determine whether it was still in use or contained known vulnerabilities.

USDA policies prohibit the use of personal use software on USDA's devices without approval documented on a personal use software request form. USDA has a long-established policy that does not condone or support employees' use of Government computers or networks for unauthorized purposes. NIST SP 800-53 Revision 4 requires that an organization establish governance for user-installed software, enforce software installation policies, and monitor its policy for compliance.

The Department should strongly discourage the use of personal use software. USDA did not enforce the personal use policy for non-mission related software. Further, the Department did not monitor personal use software for security flaws, vendor support, or security patches. There is an increased risk that software may not be supported, security flaws are not detected, and security patches are not applied or not available.

FY 2019 Recommendation 3: Enforce USDA's non-mission software policy and remove the unauthorized software from USDA systems.

There were two recommendations relating to risk management that were open and not overdue.[11] Additionally, there were two recommendations relating to risk management that were closed at the end of the audit period, and, as such, we could not determine the effectiveness of the remediation efforts.[12]

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 DR[13] that provided guidance to all agencies and staff for implementing configuration management. The Department measured the compliance of the workstations to the U.S. Government Configuration Baseline (USGCB) standards. The Department also issued DR 3530-006, *Scanning and Remediation of Configuration and Patch Vulnerabilities*, and internal Standard Operating Procedures (SOPs) related to configuration management oversight in June 2019. However, new policies and procedures take time to be fully

[11] Recommendations 1 and 6 from FISMA FY 2018.

[12] Recommendation 6 from FISMA FY 2012, and Recommendation 2 from FISMA FY 2018.

[13] DR 3520-002, *Configuration Management* (July 17, 2019).

implemented and effective. Additionally, in one of the three sampled agencies' vulnerability scans, we found a significant number of high and critical vulnerabilities, which should not be allowed in a secure baseline.

The Department adopted the Trusted Internet Connections (TIC) program to assist in protecting its network; however, the TIC program does not include security controls for mobile devices. The Department stated that there were numerous traffic flows of information outside of the TIC boundary, including mobile devices and cloud services.

There were two recommendations relating to configuration management that were closed at the end of the audit period, and, as such, we could not determine the effectiveness of the remediation efforts.[14]

Identity and Access Management (Protect)

USDA established an identity and access management program that operated at the "Consistently Implemented" maturity level. The Department developed multiple policies[15] that comprise the identity and access management program in compliance with NIST standards. Additionally, the Department adequately planned for the implementation of PIV for non-privileged and privileged access in accordance with Government standards.[16] The Department and all three agencies sampled had high percentages of PIV card usage.

The Department did not integrate all of its Identity, Credential, and Access Management (ICAM) strategy activities, such as incorporating tools from DHS CDM Phase 2 that will automate ICAM-related metrics, and an ICAM steering committee was not established as required by internal Departmental regulations in order to govern and oversee the enterprise-level ICAM approach.[17] Additionally, there was no enterprise-wide method to determine that privileged users, or those with access to sensitive information, have more specific or detailed access agreements for system use, and the Enterprise Active Directory (EAD), Enterprise Entitlements Management Service (EEMS), and CDM were still in the implementation phase.

Data Protection and Privacy (Protect)

The Department established a data protection and privacy program that operated at the "Defined" maturity level. The Department had practices related to data protection and privacy and dated policies in place;[18] however, the Department continues to lack a finalized overarching data

[14] Recommendation 2 from FISMA FY 2012, and Recommendation 5 from FISMA FY 2018.

[15] 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*.

[16] 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 allowing both physical and information technology system access.

[17] DR 3640-001, *Identity, Credential, and Access Management.*

[18] DM 3515-000, *Privacy Requirements* (Feb. 2005); DM 3515-002, *Privacy Impact Assessment* (Feb. 2005); Memo, *Minimum Safeguards for Protecting Personally Identifiable Information (PII)* (Nov. 2018).

protection and privacy policy that provides the necessary structure and direction of the privacy program and references all relevant and current NIST and OMB A-130 requirements. Additionally, there was no finalized, overarching data protection and privacy policy. The lack of updated policies and procedures led to decentralized governance of PII throughout the Department. The sampled agencies had clear practices in place; however, the practices were inconsistently implemented and reflected no overarching policy in place, and showed no evidence Departmental 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 Scorecards, Privacy Threshold Analysis, and System Privacy Summary Reports.

There was one recommendation related to data protection and privacy that was open and not overdue.[19] Additionally, there was one recommendation related to data protection and privacy that was closed at the end of the audit period, and, as such, we could not determine the effectiveness of the remediation efforts.[20]

Security Training (Protect)

The Department established a security training program that operated at a "Defined" maturity level. Policies[21] and procedures[22] met all NIST requirements for annual security awareness training. As of June 4, 2019, the Information Security Awareness (ISA) training had a completion rate of 99 percent for the three agencies sampled, OCIO, and the Department as a whole. While the Department demonstrated effective oversight of general security training, it could not determine whether specialized, tailored, and role-based security training were provided to users with significant security responsibilities or special roles. While the three agencies tested each implemented training for those with significant security responsibilities, the Department as a whole could not determine that roles and responsibilities for providing specialized, tailored, and role-based security training were appropriately resourced and consistently implemented throughout the organization.

Information Security Continuous Monitoring (ISCM) (Detect)

The Department established an ISCM program that operated at the "Defined" maturity level. The Department has a policy[23] and a strategic plan[24] for the ISCM strategy. The Department issues a biweekly scorecard, which allows for monitoring and analyzing the effectiveness of its ISCM policies and procedures. The Department did not collectively maintain a skills inventory of its workforce to determine the appropriate knowledge and skills needed to achieve its IT goals or to

[19] Recommendation 7 from FISMA FY 2018.
[20] Recommendation 13 from FISMA FY 2009.
[21] DR 3545-001, *Information Security Awareness and Training Policy* (Oct. 2013).
[22] USDA Memorandum from Tacy Summersett, CISO OCIO, *FY 2019 Mandatory Information Security Awareness (ISA) Training*, Sep. 28, 2018.
[23] DR 3540-003, *Security Assessment and Authorization* (Aug. 2014).
[24] *USDA Information Security Continuous Monitoring Strategic Plan*, Version 1.9 (Apr. 2017).

determine skills shortages or to redirect personnel to agencies or functions that require the needed expertise. The Department's Information System Owner (ISO) lacked the direct oversight of and visibility into the knowledge, skills, and abilities of the individuals needed to support the Department's IT goals.

Consequently, from an entity-wide perspective, the ISO could not ensure adequate staff and knowledge were in place to meet the objectives of the Department's ISCM program. Also, the ISCM strategy is composed of multiple programs that have not yet reached the "Consistently Implemented" maturity level, including risk management and configuration management. Additionally, the Department was still in the process of integrating all of its ISCM strategy activities, such as incorporating tools from DHS CDM Phase 2 that will automate ISCM related metrics.

Incident Response (Respond)

The Department has published Incident Response policies[25] and procedures[26] that established the Department-level Incident Response program. This program outlined response steps to security events or incidents and operated at the "Managed and Measurable" maturity level.

The policies establish the guidelines and facilitate implementation for the Department to respond to and report cybersecurity events. The Department captured and shared lessons learned on the effectiveness of policies and procedures. The Department also has a variety of metrics to monitor the effectiveness of the program (Cybersecurity Scorecards, Weekly and Monthly Activity Reports, etc.).

Open incidents older than 30 days were published on the Biweekly USDA Cybersecurity Scorecard as a metric that was visible to all of USDA. The process in place to obtain the data was well-defined and ensured the data supporting the metrics were obtained accurately, consistently, and in a reproducible format. However, the Department does not have a policy in place that fully integrates enterprise risk management with IT risk management to include the incident response program.

The Department uses DHS' EINSTEIN program for intrusion detection/prevention capabilities for traffic entering and leaving USDA's networks. The Department monitors and analyzes network traffic entering and leaving USDA's network. The Department utilizes the incident detection and prevention services provided by AT&T in partnership with DHS as part of the EINSTEIN program. Through this capability, the Department was able to detect and prevent potential compromises.

[25] DR 3505-005, *Cyber Security Incident Management* (Nov. 2018).
[26] DM 3505-005, *Cyber Security Incident Management Procedures* (Nov. 2018).

Contingency Planning (Recover)

The Department established a contingency planning program that operated at the "Defined" maturity level. A policy,[27] procedural manual,[28] and standard template[29] were established to implement the enterprise-wide business continuity/disaster recovery program. We found 42 systems for which Business Impact Analyses (BIAs) were not available in CSAM, the Department's official system of record. The results of BIA drive priorities for continuity and recovery and the strategies and resources needed to meet those priorities.

In addition, 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. A total of 67 of 327 (20 percent) operational systems did not have contingency plan testing performed within the past year.[30] 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.

There was one recommendation related to contingency planning that was open and not overdue.[31]

[27] DR 3571-001, *Information System Contingency Planning and Disaster Recovery Planning* (June 2016).
[28] *Contingency Plan Exercise Handbook*, Revision 2.1 (June 2017).
[29] *Contingency Plan Template*, v1.5 (June 2017).
[30] CSAM report as of July 30, 2019. Additionally, DR 3571-001, *Information System Contingency Planning and Disaster Recover Planning* (June 2016), states that contingency plans shall be tested at least annually.
[31] Recommendation 8 from FISMA FY 2018.

Scope and Methodology

Scope

The scope of our review was Departmentwide. In total, our FY 2019 FISMA audit work covered four agencies and offices:

- Agricultural Research Service (ARS);
- Foreign Agricultural Service (FAS);
- Food and Nutrition Service (FNS); and
- OCIO.

As of August 15, 2019, these agencies and offices operated 75 of the Department's 328 operational systems.

Methodology

The audit was designed to determine whether the Department implemented certain security controls for selected information systems in support of the Federal Information Security Modernization Act of 2014. Our audit was conducted for FY 2019 and consisted of testing the 67 FISMA Reporting Metrics issued by DHS.

We conducted this audit in accordance with Generally Accepted Government Auditing Standards (also known as the Yellow Book)[32] issued by the Comptroller General of the United States. 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 SP 800-53A Revision 4, *Guide for Assessing Security Controls in Federal Information Systems and Organizations;* NIST SP 800-53 Revision 4, *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 for each of the eight domains by a simple majority of the maturity level competent scores for each question within the domain, in accordance with the *FY 2019 IG FISMA Reporting Metrics Version 1.3.*

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

[32] GAO Government Auditing Standards (2011 Revision).

Abbreviations

AAR	Acquisition Approval Request
AC	access control
AM	asset management
ARS	Agricultural Research Service
ASOD	Agriculture Security Operations Division
AT	awareness and training
ATO	Authorization to Operate
BE	business environment
BIA	Business Impact Analysis
BOD	Binding Operational Directive
CA	Security Assessment and Authorization
CCB	Change Control Board
CDM	Continuous Diagnostics and Mitigation
CEC	Client Experience Center
CFO	Chief Financial Officer
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CM	configuration management
CO	communications
CP	contingency planning
CSAM	Cyber Security Assessment Management System
CSF	Cybersecurity Framework
CSIP	Cybersecurity Strategy and Implementation Plan
CSIRT	Computer Security Incident Response Team
CVSS	Common Vulnerability Scoring System
DE	Detect
DE.AE	anomalies and events (Detect)
DE.CM	Security Continuous Monitoring (Detect)
DE.DP	detection processes (Detect)
DHS	Department of Homeland Security
DM	Departmental Manual
DR	Departmental Regulation
EAD	Enterprise Active Directory
ED	emergency directive
EEMS	Enterprise Entitlements Management Service
ERM	Enterprise Risk Management
FAS	Foreign Agricultural Service
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
FMFIA	Federal Managers' Financial Integrity Act
FNS	Food and Nutrition Service
FY	fiscal year
GAO	Government Accountability Office
GV	governance
HVA	High Value Asset
HSPD	Homeland Security Presidential Directive
IA	identification and authentication
ICAM	Identity Credential and Access Management
ISA	Information Security Awareness
ISO	Information System Owner
ID	Identify
ID.AM	asset management (Identify)
ID.BE	business environment (Identify)
ID.GV	governance (Identify)
ID.RA	risk assessment (Identify)
ID.RM	Risk Management Strategy (Identify)
ID.SC	Supply Chain Risk Management (Identify)
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
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	personally identifiable information
PIV	Personal Identity Verification
PL	planning
PM	program management
POA&M	Plan of Action and Milestones
PPD	Presidential Policy Direction
PR	Protect
PR.AC	Identity Management and Access Control (Protect)
PR.AT	awareness and training (Protect)
PR.DS	data security (Protect)
PR.IP	Information Protection Processes and Procedures (Protect)
PR.PT	protective technology (Protect)
PS	personnel security
RA	risk assessment

RC	Recover
RC.CO	communications (Recover)
RM	Risk Management Strategy
RMF	Risk Management Framework
ROB	Rules of Behavior
RS	Respond
RS.AN	analysis (Respond)
RS.CO	communications (Respond)
RS.MI	mitigation (Respond)
RS.RP	response planning (Respond)
SA	System and Services Acquisition
SANS	Sysadmin, Audit, Network, Security
SDLC	Systems Development Life Cycle
SI	System and Information Integrity
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SOP	Standard Operating Procedure
SP.	Special Publication
SSP	System Security Plan
TIC	Trusted Internet Connections
US-CERT	United States Computer Emergency Readiness Team
USDA	Department of Agriculture
USGCB	United States Government Configuration Baseline

Criteria

We focused our FISMA audit approach on Federal information security guidelines developed by DHS, NIST, and OMB. NIST Special Publications provide guidelines that are considered essential to the development and implementation of the Department's security programs. The following is a list of the criteria used in the performance of the FY 2019 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*
- 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 19-02, *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements*
- OMB Memorandum M-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*
- 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 (CISP) for the Federal Civilian Government*
- OMB Memorandum M-08-05, *FY 2008 Implementation of Trusted Internet Connections (TIC)*
- OMB Circular A-130, *Managing Information as a Strategic Resource*

Department of Homeland Security

- *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.3 April 9, 2019*

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

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 /s/
Chief Information Officer
Office of the Chief Information Officer

SUBJECT: Office of Inspector General Audit 50503-0002-12, *Fiscal Year 2019 Federal Information Security Modernization Act Audit*

The Office of the Chief Information Officer (OCIO) has reviewed the draft report and generally agrees with the Office of Inspector General's (OIG) assessment of the Department's Information Technology security program. We also appreciate the opportunity to provide comments on this draft report for your consideration.

Internally, OCIO has a robust and effective cybersecurity policy program. The policy program conducts a complete review of the directives annually and reprioritizes the list of directives to update or write based on OIG findings. Items that are updated include: plans of action and milestones, waivers, feedback received from agency and Department personnel, and input from the Directives team. Our biggest challenge has typically been due to the lengthy review and approval process. Despite this, our team excelled by publishing seven Directives, many of which have contributed to the closure of aged audit recommendations. With our shared goals in mind, we strive to ensure that the United States Department of Agriculture (USDA) personnel are empowered with current Directives. To enhance these efforts in FY20, we will be augmenting our policy writing staff, and will continue to press for Directive drafts to be reviewed in a timely manner.

OCIO will continue to improve its security posture in FY20 by further centralizing all security operations for USDA Department and Mission Areas through the USDA's Security Operations (SecOps) Consolidation project, and by continuing to implement Continuous Diagnostics and Mitigation (CDM). Part of the CDM effort includes application scanning of systems at all levels to safeguard against unauthorized software.

The OCIO appreciates the work of the OIG in conducting its review and issuing this report. OCIO will utilize OIG's assessment to continue to strengthen management and technical controls over its Information Technology security programs.

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

Cc: Venice M. Goodwine, OCIO, Chief Information Security Officer
Tacy Summersett, OCIO, Deputy Chief Information Security Officer
Annie Walker-Bradley, OCFO, Director, Internal Control Division
Lynn Moaney, OCFO, Associate Chief Financial Officer
Lance Moore, OIG, Assistant Regional Inspector General
Tonya Judkins, OCIO Chief of Staff
Terence Goodman, Director, Security Management Division
Martin Kihiko, Chief, Security Services Branch
Benjamin Moreau, Chief, Compliance and Policy Branch

Learn more about USDA OIG
Visit our website: **www.usda.gov/oig**
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

Bribery / Assault
202-720-7257 (24 hours)

All photographs on the front and back covers are from USDA's Flickr site and are in the public domain. They do not depict any particular audit or investigation.