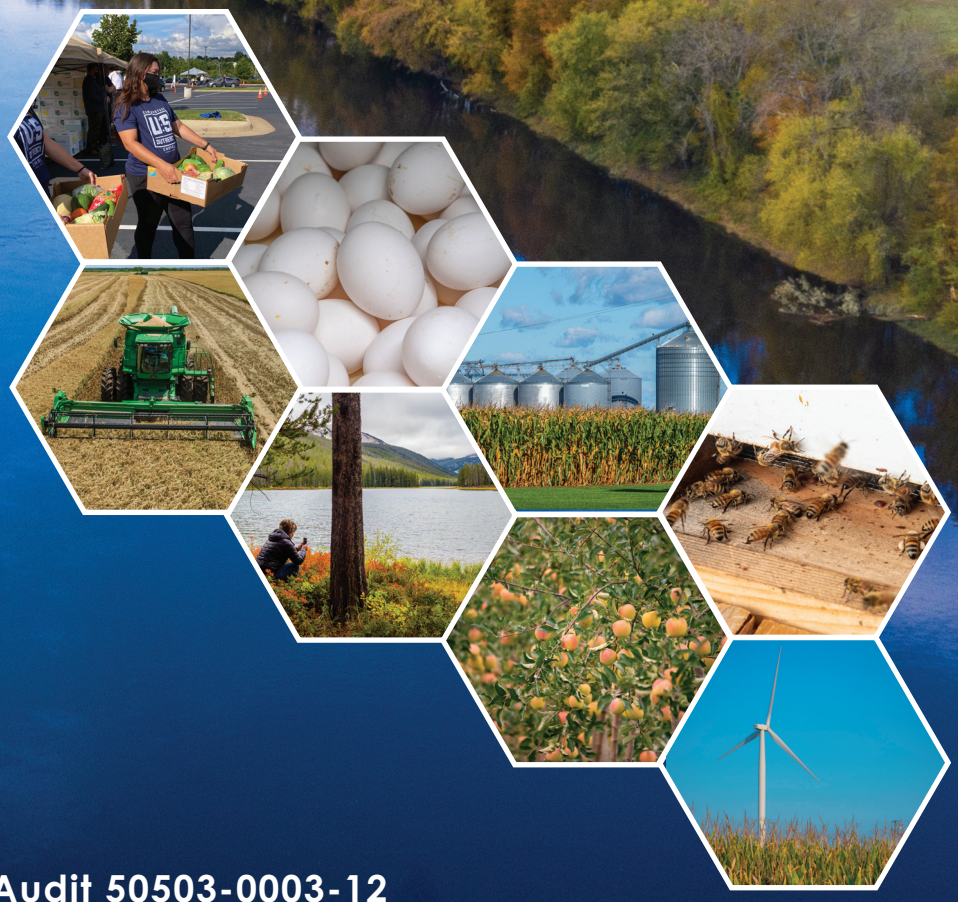
USDA
United States Department of Agriculture

U.S Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2020 Federal Information Security Modernization Act



Audit 50503-0003-12

October 2020

OFFICE OF INSPECTOR GENERAL

IMPORTANT NOTICE

This report contains sensitive content. Sections of this report are being withheld from public release due to concerns about the risk of circumvention of law.

U.S Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2020 Federal Information Security Modernization Act

Audit Report 50503-0003-12

As required by FISMA, OIG reviewed USDA's ongoing efforts to improve its information technology security program and practices during FY 2020. -

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

REVIEWED

The scope was Departmentwide, and we reviewed agency IT audit work completed during FY 2020. This audit covered four agencies and offices operating 129 of the Department's 329 operational systems.

RECOMMENDS

We recommend the Department mitigate existing security weaknesses by developing policy and implementing procedures; implementing a centrally managed software license program; prioritizing the remediation of outstanding vulnerabilities; removing unsupported software; revising regulations; implementing an improved patch and upgraded process; and implementing mechanisms and controls to ensure system contingency plans are tested annually, among other recommendations.

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) 2009–2019, there were 14 outstanding recommendations that remain unresolved—11 recommendations are completed, and 3 recommendations are scheduled for closure after the date of our report. We have also issued nine new recommendations based on security weaknesses identified in FY 2020.

The Office of Management and Budget establishes standards for an effective level of security and considers "Managed and Measurable" to be a sufficient level. However, we found the Department's maturity level to be at the "Consistently Implemented" level. Based on OMB's criteria, the Department's overall score indicates an ineffective level of security. In our detailed testing of the 67 Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics, we found the Department increased its maturity level for 5 metrics. Seven metrics' maturity level was downgraded because of a new requirement related to supply chain risk management and the most recent cyber incidents. The maturity level did not change for 55 metrics. The Department and its agencies must develop and implement an effective plan to mitigate security weaknesses identified in the prior fiscal year recommendations. OCIO generally concurred with the findings and recommendations in the report.

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 29, 2020

AUDIT NUMBER: 50503-0003-12

TO: Gary S. Washington
Chief Information Officer
Office of the 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 2020 Federal Information Security Modernization Act

This report presents the results of the subject review. The instructions for fiscal year (FY) 2020 Federal Information Security Modernization Act (FISMA) are outlined in the *FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, v4.0, dated April 17, 2020. This report contains our responses to the questions contained in these instructions. Your written response to the draft is included in its entirety at the end of the report. Corrective actions plans for the recommendations contained in the report should be provided to the Office of Inspector General within 60 days of this report date.

We appreciate the courtesies and cooperation extended to us by members of your staff during our 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

United States Department of Agriculture
Federal Information Security Modernization Act of 2014
Audit Report for Fiscal Year 2020

RMA | Associates
Auditors. Consultants. Advisors.

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

October 28, 2020

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

Re: U.S. Department of Agriculture, Federal Information Security Modernization Act of 2014 Audit Report for Fiscal Year 2020

Dear Ms. Fong:

RMA Associates, LLC is pleased to submit the United States Department of Agriculture (USDA or Department) Federal Information Security Modernization Act of 2014 (FISMA) Audit Report for Fiscal Year (FY) 2020. 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 2020 Inspector General FISMA Reporting Metrics Version 4. 0* (April 17, 2020) as a separate deliverable. 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 2020.

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, LLC
Arlington, VA

RMA Associates
Auditors. Consultants. Advisors.

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

United States Department of Agriculture
Federal Information Security Modernization Act of 2014
Audit Report for Fiscal Year 2020

Table of Contents

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

Background

The United States Department of Agriculture (USDA or Department) relies extensively on information technology (IT) resources to accomplish its mission. The IT systems and resources strengthen the management and oversight of the Department's procurement, property, and finances to ensure resources are used 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 sharing of information instantaneously among stakeholders, 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.

Key Changes to the Fiscal Year (FY) 2020 Inspector General (IG) Federal Information Security Modernization Act Of 2014 (FISMA) Metrics

One of the goals of the annual FISMA evaluation 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 2020 Chief Information Officer (CIO) FISMA Metrics* include an additional focus on the security of mobile devices (Government-furnished equipment (GFE) and non-GFE), particularly in the areas of mobile device management and enterprise mobility management. As such, the *FY 2020 IG FISMA Reporting Metrics* include updates to questions on asset management, security architecture, and flaw remediation (Questions 2, 3, 6, and 19) to assess agency progress in securing mobile endpoints and employing secure application development processes.

Furthermore, the Office of Management and Budget (OMB) has issued updated guidance on the Trusted Internet Connection (TIC) initiative. Specifically, OMB Memorandum M-19-26, *Update to the Trusted Internet Connections (TIC) Initiative* (September 12, 2019), provides updated guidance to Federal agencies on the use of TIC capabilities in modern architectures and frameworks, such as cloud-based infrastructures. While the memorandum gives agencies until September 12, 2020, to implement new TIC requirements, the IG FISMA metrics on TIC implementation (Question 20) have been updated to assess the agency's progress in planning for the effective implementation of the security capabilities outlined in M-19-26.

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*. Title III required 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.

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

On December 18, 2014, the President signed 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 reduce overall reporting, strengthen the use of continuous monitoring in systems, increase focus on the agencies for compliance, and produce reporting on more focused issues caused by security incidents.

FISMA requires Federal agencies to have an annual, independent assessment of their information security program and practices performed to determine the effectiveness of such program and practices, and to report the results of the assessment to 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 the 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 time of, major incidents; (3) detection, response, and remediation actions; (4) 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

[1] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 2014), https://www.congress.gov/bill/113th-congress/senate-bill/2521.
[2] Ibid.
[3] Ibid.
[4] Ibid.
[5] Ibid.

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

information security standards and guidelines. NIST developed an integrated Risk Management Framework that effectively brought together all of 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:[6]

- 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. This support includes assessing risk, determining the levels of information security, implementing policies to reduce risks cost-effectively, and periodically testing and evaluating security controls.

FISMA requires the Office of Inspector General (OIG) 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.[7]

FISMA Reporting Metrics

The *FY 2020 IG FISMA Reporting Metrics*[8] 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 CIO Council. The FY 2020 metrics represent a continuation of work begun in FY 2016 when the IG metrics[9] 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 2020 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] Ibid.
[7] NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Apr. 2013, updated Jan. 22, 2015.
[8] *FY 2020 IG FISMA Reporting Metrics v4.0* (Apr. 2020).
[9] *FY 2016 IG FISMA Reporting Metrics v1.1.3* (Sep. 2016).

1005 N. Glebe Road, Suite 610
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 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 the high-value asset (HVA)[10], mobile devices, 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 are not formalized; activities are performed in an ad hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategies are formalized and documented, but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess them and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

The *FY 2020 IG FISMA Reporting Metrics* states that the "Managed and Measurable" level represents an effective information security program.

[10] An HVA is information or an information system that is so critical to an organization that the loss or corruption of this information or loss of access to this system would have serious impact on the organization's ability to perform its mission or conduct business.

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

DHS' CyberScope website captures agencies' consolidated reporting results. Each Cybersecurity Framework security function area assigns 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 (ISCM);
- **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 Exhibit 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, as listed in Exhibit B.

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

U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2020 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 2020 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 FY 2020 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 the 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 its IT infrastructure and services. The Department focused on improving the efficiency and effectiveness of its management activities across the Department and centralizing business functions in each mission area to help ensure better alignment.

Per the FY 2019–2022 OCIO Information Technology Strategic Plan, OCIO is supporting multiple strategic themes:

- Strengthen strategic IT governance;
- Consolidate end user services and infrastructure optimization;
- Enable strategic approach to data management and data-driven capabilities;
- Improve USDA customer experience; and
- Accelerate cloud adoption.[11]

[11] FY 2019–2022 OCIO Information Technology Strategic Plan, https://www.ocio.usda.gov/strategic-plan.

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

Although the Department has demonstrated a concerted effort to close many of the outstanding recommendations in FY 2020, significant security weaknesses still exist. During the current year, the Department completed corrective actions by revising its policies and procedures for compliance 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. Also, some prior recommendations remain open, and our current year testing found additional security weaknesses.

The Department's overall maturity level increased to Level 3: "Consistently Implemented." At Level 3, policies, procedures, and strategies are formalized and documented, and they are consistently implemented; however, the ISCM and contingency planning are at Level 2: "Defined." At Level 2, policies, procedures, and strategies are formalized and documented but not consistently implemented. Also, data protection and privacy are at Level 1: "Ad Hoc." At Level 1, policies, procedures, and strategies are not formalized; activities are performed in an ad hoc, reactive manner.

DHS considers information security programs to be 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 level of "Consistently Implemented," we reported 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 five metrics. Seven metrics' maturity level was downgraded because of the requirements related to supply chain risk management and the most recent cyber incidents. Also, the maturity level did not change for 55 metrics.

The 67 FISMA Reporting Metrics are grouped into four functions and eight domains. For the FY 2020 FISMA, the maturity level for the four functions are shown below:

Table 2: The Department's Maturity Levels

Function	Maturity Level	
Function 1: Identify—Risk Management		Consistently Implemented (Level 3)
Function 2: Protect		Consistently Implemented (Level 3)
• Configuration Management	Consistently Implemented (Level 3)	
• Identity Management	Consistently Implemented (Level 3)	
• Data Protection and Privacy	Ad Hoc (Level 1)	
• Security Training	Defined (Level 2)	
Function 3: Detect—Information Security Continuous Monitoring		Defined (Level 2)

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

Function	Maturity Level
Function 4: Respond—Incident Response	Managed and Measurable (Level 4)
Function 5: Recover—Contingency Planning	Defined (Level 2)
Overall	**Not Effective**

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 it is to allow individual agencies to manage these control activities.

USDA worked extensively in FY 2020 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 conducted from 2009 through 2019, at the beginning of FY 2020, there were 14 outstanding recommendations. During FY 2020, 11 recommendations were closed (see Exhibit B). We acknowledge that OCIO made a concerted effort to close many of the outstanding recommendations.

For FY 2020, RMA issued nine recommendations. OCIO generally agreed with our findings and recommendations. See *Agency's Response to Audit Report* in Exhibit C for OCIO's response in its entirety.

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 the Departmental Cyber Security Assessment Management System (CSAM), more centralized oversight is needed. Due to decentralized 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 implement its strategic plan, to consolidate common IT functions into a central corporate model and improve the oversight of the agencies' compliance with Departmental policies.

Exhibit A contains our responses to the OMB/DHS/CIGIE FY 2020 FISMA security questions. These questions are defined on the DHS CyberScope FISMA reporting website. The following paragraphs summarize the key matters discussed in Exhibit A of this report.

Risk Management (Identify)

The Department increased the maturity level of its Risk Management program from last year as "Ad Hoc" to this year as "Consistently Implemented."

Improvements are still needed. Our testing noted the Department's policies and procedures did not address its responsibilities for cloud services related to Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). For example, for some cloud systems, the Department is not responsible for risk assessments (RA), authorization to

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

operate (ATO), or contingency planning (CP). The Department relies on the cloud system's Federal Risk and Authorization Management Program (FedRAMP) certification instead of performing Ras, ATOs, and CPs. The Department has adopted a practice of creating a "Front End" system security program (SSP) to define the Department's responsibilities for cloud systems. The Department's responsibilities differ depending on the type of cloud service provided.

We found that information in CSAM was inconsistent and summary reports did not agree with detailed supporting artifacts. In reviewing reports at the Department-level, the Department cannot determine whether it is compliant with Federal regulations.

- **FY 2020 Recommendation 1:** We recommend the Department develop a policy and implement the necessary oversight to monitor CSAM for accuracy so that the system provides sufficient support to determine compliance with Federal requirements and for decision making.

OCIO is responsible for overseeing the software license program and whether the program is functioning according to Departmental policies. The policies require OCIO to reconcile purchased software licenses to those licenses that are installed on Department computer systems. However, the Department does not have an entity-wide system for reviewing and managing its software licenses.

- **FY 2020 Recommendation 2:** We recommend the Department implement a centrally managed software license program that complies with Departmental policy.

The Department did not have an approved Supply Chain Plan that would establish the strategies to mitigate the risks associated with information and communications technology (ICT) products and services. These risks may decrease visibility into, understanding of, and control over how the technology that they acquire is developed, integrated, and deployed, as well as the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of the products and services.

A recommendation addressing this weakness will be issued under another auditor's report. Therefore, we are not issuing a new recommendation.[12]

[12] RMA coordinated the report with OIG related to other ongoing audits to avoid issuing a duplicate recommendation for the lack of a supply chain plan as the *GAO-20-481SU, Information and Communications Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks,* is to issue a similar recommendation.

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

There were five recommendations related to risk management: two closed,[13] one open,[14] and two overdue.[15] OCIO also closed six recommendations that were related to governance structure and vulnerability management.[16]

Configuration Management (Protect)

The Department increased the maturity levels of its Configuration Management program from last year as Defined to this year as Consistently Implemented.

However, our testing noted the Department did not have an effective process for remediating known vulnerabilities on IT devices in a timely manner. The Departmental Regulation (DR) 3530-006, *Scanning and Remediation of Configuration and Patch Vulnerabilities* (June 2019), state that critical vulnerabilities must be corrected within 14 days. All vulnerabilities rated as high, moderate, or low risk will be remediated within 30 days, or have a plan of action and milestones (POA&M) created and managed in the Department's official system of record in accordance with DR 3565-003, *Plan of Action and Milestones Policy* (Sept. 2013). DR 3565-003*, Plan of Action and Milestones Policy* (Sept. 2013), does not specify the time required for resolving vulnerabilities. The longer the known vulnerability is exposed on the network, the greater the risk that the vulnerability could be exploited.

We reviewed network vulnerability scans for the selected agencies and the independent scans performed by OIG and Security Information and Event Management (SIEM). We found a significant number of critical network vulnerabilities that were not remediated within 14 days, unsupported software, and unapplied patches or upgrades. Also, vulnerabilities rated as high, moderate, or low risk were not recorded in CSAM, the system of record. Additionally, we found a significant number of high vulnerabilities on the selected agencies' public-facing websites that were unknown to the agencies.

- **FY 2020 Recommendation 3:** We recommend the Department prioritize remediation of outstanding vulnerabilities to address security and control deficiencies by implementing an improved patch or upgrade process to address security deficiencies identified by the independent OIG scans and SIEM.

- **FY 2020 Recommendation 4:** We recommend the Department remove unsupported software from its network by designing and implementing a strategic Departmentwide plan.

[13] Recommendations 2 and 3 from FISMA FY 2019 (50503-002-12). RMA required more time to perform detail testing. As a result, we will test the implementation of this recommendation in FY 2021.
[14] Recommendation 1 from FISMA FY 2019 (50503-002-12).
[15] Recommendations 6 and 7 from FISMA FY 2018 (50501-0018-12).
[16] Recommendations 6 from FISMA FY 2012 (50501-0003-12), 1 from FISMA FY 2016 (50501-0012-12) and 2, 3, 4, and 5 from FISMA FY 2018 (50501-0018-12).

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

- **FY 2020 Recommendation 5:** We recommend the Department revise the DR 3565-003, *Plan of Action and Milestones Policy* to specify a timetable or time constraint for resolving high, medium and low vulnerabilities.

- **FY 2020 Recommendation 6:** We recommend the Department implement an improved patch and upgraded process to address security deficiencies identified by the independent OIG scans and SIEM.

Identity and Access Management (Protect)

The Department established an identity and access management program that operated at the "Consistently Implemented" maturity level, the same maturity level as last year. The Department developed multiple policies[17] that comprise the identity and access management program in compliance with NIST 800-53 Rev. 4 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.[18] The PIV card usage across the Department was at 95 percent.

However, the Department did not integrate all of its identity, credential, and access management (ICAM) strategy activities, such as incorporating tools from DHS Continuous Diagnostic Monitoring (CDM) Phase 2 that will automate ICAM-related metrics, and an ICAM steering committee was not established, as required by internal DRs, in order to govern and oversee the enterprise-level ICAM approach.[19]

- **FY 2020 Recommendation 7:** We recommend the Department incorporate tools from DHS CDM Phase 2 and establish an ICAM steering committee to oversee the enterprise-level ICAM approach.

Data Protection and Privacy (Protect)

The Department established a data protection and privacy program that operated at the "Ad Hoc" maturity level, the same maturity level as last year. The Department had practices related to data

[17] DR 3640-001, *Identity, Credential, and Access Management*, Dec. 9, 2011, https://www.ocio.usda.gov/document/departmental-regulation-3640-001; DR 3505-003, *Access Control for Information and Information Systems*, July 17, 2019, https://www.ocio.usda.gov/document/departmental-regulation-3505-003; DR 4620-002, *Common Identification Standard for U.S. Department of Agriculture*, Sep. 29, 2014, https://www.ocio.usda.gov/document/departmental-regulation-4620-002.

[18] The Executive Branch mandate entitled, *Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors (*Aug. 27, 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 IT system access.

[19] DR 3640-001, *Identity, Credential, and Access Management*, Dec. 9, 2011, https://www.ocio.usda.gov/document/departmental-regulation-3640-001.

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

protection and privacy and antiquated policies in place.[20] The Department continued to lack a finalized, overarching data 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. The lack of updated policies and procedures led to decentralized governance of personally identifiable information (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 no evidence that 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. Also, the Department did not consistently sanitize decommissioned hardware devices and did not retain the sanitization certifications.

- **FY 2020 Recommendation 8:** We recommend the Department implement the policy and procedures related to media sanitization. In addition, the Department should consistently perform sanitization of decommissioned hardware devices and maintain the sanitization certifications.

There was one recommendation related to data protection and privacy that was closed.[21] OCIO also closed one recommendation that was related to OMB Privacy Memos.[22]

Security Training (Protect)

The Department established a security training program that operated at the "Defined" maturity level, the same maturity level as last year. Policies[23] and procedures met all NIST requirements for annual security awareness training. As of June 2020, the information security awareness (ISA) training had a completion rate of 97 percent for the three agencies sampled, OCIO, and the Department as a whole. RMA concluded that all three agencies implemented and tracked the completion of specialized security training for those individuals with significant security responsibilities; however, the Department does not have insight into the requirements established by each agency concerning the positions that require additional training. The Department has given the agencies a due date of May 30, 2021, to develop security awareness and specialized training policies and procedures and provide them to Property Management Division (PMD) for review and analysis; therefore, we are not making a recommendation in this area.

---

[20] Departmental Manual (DM) 3515-000, *Privacy Requirement*s, Feb. 17, 2005, https://www.ocio.usda.gov/document/departmental-manual-3515-000; DM 3515-002, *Privacy Impact Assessment*, Feb. 17, 2005, https://www.ocio.usda.gov/document/departmental-manual-3515-002; Memo, *Minimum Safeguards for Protecting Personally Identifiable Information (PII)* (Aug. 2016).

[21] Recommendation 1 from FISMA FY 2018 (50501-0018-12). RMA required more time to perform detail testing. As a result, we will test the implementation of this recommendation in FY 2021.

[22] Recommendation 8 from FISMA FY 2009 (50501-15-FM).

[23] DR 3545-001, *Information Security Awareness and Training Policy*, Oct. 22, 2013, https://www.ocio.usda.gov/document/departmental-regulation-3545-001.

1005 N. Glebe Road, Suite 610
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, the same maturity level as last year.

The Department established policy[24] and a strategic plan[25] for the ISCM strategy. The Chief Human Capital Officers Council (CHCOC) monitored and assessed IT workforce knowledge and skills needed to achieve the Department's IT goals. The Department was scheduled to have a human capital review for FY 2020; however, due to COVID-19, the review was canceled.

However, 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. Therefore, we are not making a recommendation in this area.

Incident Response (Respond)

The Department has published Incident Response policies[26] and procedures[27] that established the Department level incident response program, which outlined response steps to security events or incidents. The response program operated at the "Managed and Measurable" maturity level, the same maturity level as last year.

The policies established 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 had a variety of metrics to monitor the effectiveness of the program (weekly and monthly activity reports).

The incident activities were published on the Department's internal dashboard that was visible to all of USDA. The process in place to obtain the data was well-defined, ensuring the data supporting the metrics were obtained accurately, consistently, and in a reproducible format. However, the Department did not have a policy in place that fully integrated enterprise risk management with IT risk management to include the incident response program.

[24] DR 3540-003, *Security Assessment and Authorization*, Aug. 12, 2014, https://www.ocio.usda.gov/document/departmental-regulation-3540-003.
[25] *USDA Information Security Continuous Monitoring Strategic Plan*, Version 1.9, Apr. 2017.
[26] DR 3505-005, *Cybersecurity Incident Management,* Nov. 30, 2018, https://www.ocio.usda.gov/document/departmental-regulation-3505-005.
[27] DM 3505-005, *Cybersecurity Incident Management Procedures*, Nov. 30, 2018, https://www.ocio.usda.gov/document/departmental-manual-3505-005.

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

The Department uses DHS' EINSTEIN program[28] for intrusion detection/prevention capabilities for traffic entering and leaving the Department's networks. The Department monitors and analyzes network traffic entering and leaving the Department'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.

Contingency Planning (Recover)

The Department established a contingency planning program that operated at the "Defined" maturity level, the same maturity level as last year. A policy,[29] procedural manual,[30] and standard template[31] were established to implement the enterprise-wide business continuity/disaster recovery program. We found that, for 30 out of 329[32] systems, the business impact analysis (BIA) was 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 329 (20 percent) operational systems did not have contingency plan testing performed within the past year.[33] Testing of system contingency plans is critical to ensuring effective system contingency plans are in place. Without effective system contingency plans, the Department's mission data is at a higher risk of loss due to an unscheduled disruption. Specifically, unscheduled disruptions in operations may debilitate the Department in such a way that it may be unable to recover and continue operations of all necessary systems and functions in a timely manner.

- **FY 2020 Recommendation 9:** We recommend the Department design and implement the necessary oversight and enforcement mechanisms and controls to ensure all system contingency plans are tested annually. The results of all tests should be reviewed annually to ensure corrective actions can be initiated, as necessary.

[28] DHS EINSTEIN program detects and blocks cyber-attacks from compromising federal agencies. Also, it provides DHS situational awareness to use threat information detected in one agency to protect the rest of the government (https://www.cisa.gov/einstein).
[29] DR 3571-001, *Information System Contingency Planning and Disaster Recovery Planning*, June 1, 2016, https://www.ocio.usda.gov/document/departmental-regulation-3571-001.
[30] *Contingency Plan Exercise Handbook*, Revision 2.1, June 2017.
[31] *Contingency Plan Template*, v1.5, June 2017.
[32] As of the CSAM report (July 2020), there were a total of 329 FISMA reportable systems in operation at the Department level.
[33] CSAM report as of (June 2020). Additionally, DR 3571-001, *Information System Contingency Planning and Disaster Recover Planning* (June 2016), states that contingency plans shall be tested at least annually.

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

There was one recommendation related to contingency planning that was closed.[34]

[34] Recommendation 8 from FISMA FY 2018 (50501-0018-12). RMA required more time to perform detail testing. As a result, we will test the implementation of this recommendation in FY 2021.

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

Scope and Methodology

Scope

The scope of our review was Departmentwide. In total, our FY 2020 FISMA audit work covered four agencies:

- Forest Service (FS);
- Farm Service Agency (FSA);
- Food Safety and Inspection Services (FSIS); and
- OCIO.

As of August 21, 2020, the selected agencies operated 129 of the Department's 329 operational FISMA reportable systems.[35]

Methodology

The audit was designed to determine whether the Department implemented selected security controls for selected information systems in support of FISMA. Our audit was conducted for FY 2020 and consisted of testing the 67 FISMA Reporting Metrics issued by DHS.

The overall strategy of our audit considered NIST Special Publication (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 2020 IG FISMA Reporting Metrics Version 4.0.*

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 also inspected OIG's network scanning reports. We considered the 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 and followed up on applicable GAO engagements.[36]

We conducted this audit in accordance with Generally Accepted Government Auditing Standards (also known as the Yellow Book)[37] 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

[35] Certain controls were tested at the agency level and some controls were tested at the Department level.
[36] RMA coordinated the report with OIG related to other ongoing audits to avoid issuing a duplicate recommendations as some GAO reports may issue a similar recommendations.
[37] GAO Government Audit Standards (2018 Revision).

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

objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

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

Abbreviations

AAR .....acquisition approval request
ATO .....authorization to operate
BIA.....business impact analysis
CAP.....corrective action plan
CCB.....Change Control Board
CDM .....continuous diagnostics and mitigation
CHCOC.....Chief Human Capital Officers Council
CIGIE.....Council of the Inspectors General on Integrity and Efficiency
CIO.....Chief Information Officer
CISO .....chief information security officers
CISP .....cybersecurity strategy and implementation plan
CP.....contingency planning
CRO .....chief risk officer
CSAM .....Cyber Security Assessment Management System
CVSS.....Common Vulnerability Scoring System
DHS.....Department of Homeland Security
DISA .....Defense Information Systems Agency
DISC .....Digital Infrastructure Services Center
DM .....departmental manual
DR .....departmental regulation
DRP.....Disaster Recovery Plan
EAD .....Enterprise Active Directory
EEMS.....Enterprise Entitlements Management Service
ERM.....enterprise risk management
FedRAMP .....Federal Risk and Authorization Management Program
FIPS.....Federal Information Processing Standards
FISMA .....Federal Information Security Modernization Act of 2014
FMFIA .....Federal Managers' Financial Integrity Act
FS .....Forest Service
FSA .....Farm Service Agency
FSIS.....Food Safety and Inspection Services
FY .....fiscal year
GAO.....Government Accountability Office
GFE.....Government-furnished equipment
HVA .....high-value asset
IaaS .....Infrastructure as a Service
ICAM .....identity credential and access management
ICT .....information and communications technology
ISA .....information security awareness
ISC .....information security center
ISO .....information system owner
IG .....Inspector General
ISCM.....information security continuous monitoring
IT.....information technology

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

NDA.....nondisclosure agreements
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
PaaS.....Platform as a Service
PII.....personally identifiable information
PIV .....personal identity verification
PMD.....Property Management Division
POA&M.....plan of action and milestones
RA .....risk assessment
RMF .....risk management framework
ROB .....rules of behavior
SaaS.....Software as a Service
SDLC .....systems development life cycle
SECURE .....Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure
SIEM .....security information and event management
SLAs .....service-level agreements
SP .....special publication
SSP.....system security program
STIG.....Security Technical Implementation Guide
TIC .....trusted internet connection
USDA.....United States Department of Agriculture
USGCB .....United States Government Configuration Baseline

1005 N. Glebe Road, Suite 610
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 SPs provide guidelines that were 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 2020 FISMA audit:

NIST Federal Information Processing Standards (FIPS) and SPs

- 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*

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

- NIST SP 800-181, *NICE Cybersecurity Workforce Framework*

OMB Policy Directives

- OMB Memorandum M-20-04 *Fiscal Year 2019–2020 Guidance on Federal Information Security and Privacy Management Requirements*
- OMB Memorandum M-19-26, *Update to the Trusted Internet Connections (TIC) Initiative*
- 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-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 Circular No. A-130, *Managing Information as a Strategic Resource*

DHS

- FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 4.0 April 17, 2020

In addition to the above criteria, we compared the security practices to the Department's internal policies and procedures.

The subsequent sections of this report, “Exhibit A” and “Exhibit B”, are not being publicly released due to the sensitive security content.

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

Exhibit C – Agency's Response to Audit Report

United States Department of Agriculture

Office of the Secretary

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 the Inspector General

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

SUBJECT: Office of Inspector General Audit #50503-0003-12, Fiscal Year 2020 "Federal Information Security Modernization Act"

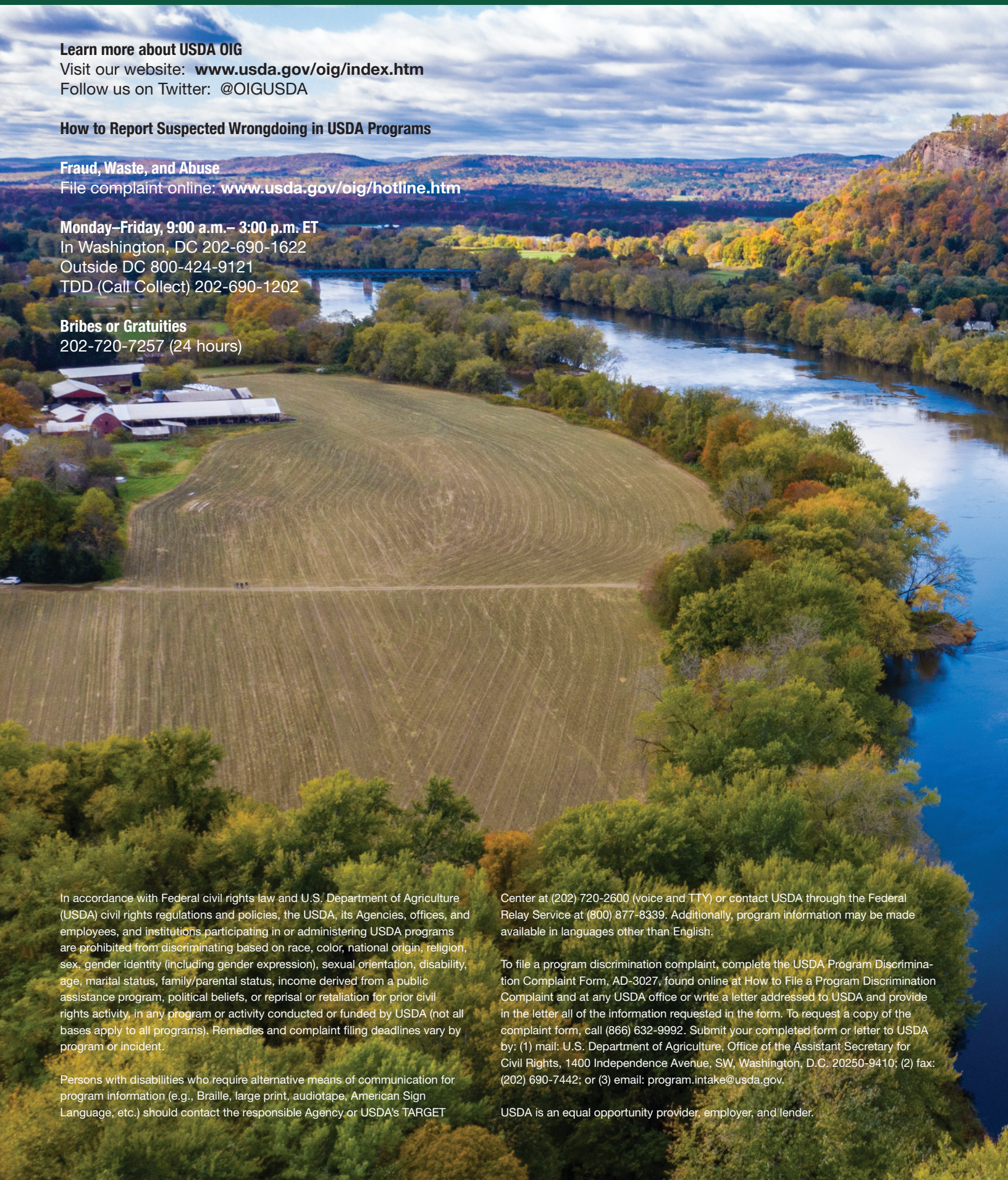
The Office of the Chief Information Officer (OCIO) has reviewed the Office of the Inspector General's (OIG) draft report, "Federal Information Security Modernization Act Audit", Fiscal Year 2020 #50503-0003-12 and generally concurs with the findings and recommendations in the report.

OCIO will work with Mission Area Assistant Chief Information Officers (ACIOs) and key OCIO stakeholders to develop our Management Decision which will include our specific plan of action and milestones to assess, design, and implement solutions.

We look forward to receiving the final OIG report.

If additional information is needed, please contact Megen Davis, OCIO Audit Liaison, at (202) 631-1266.

cc: Megen Davis, Audit Liaison, OCIO
Mohammad Nikravesh, Audit Liaison
Maria Vlioras, Executive Assistant, CIO
Venice Goodwine, Chief Information Security Officer (CISO), OCIO
Brittany Smith, Executive Assistant, CISO, OCIO
Benjamin Moreau, Director, Security Management Division (Acting), ISC
LaTonya Finch, IT Security Specialist, ISC



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)