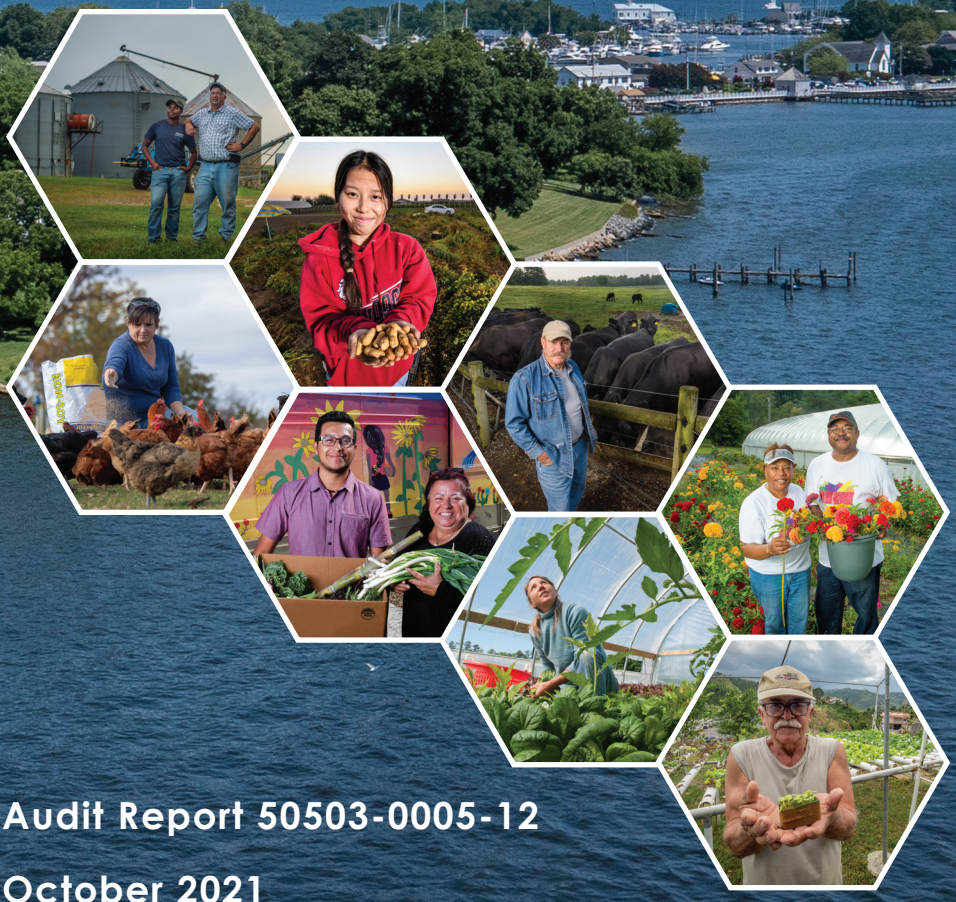
USDA OFFICE OF INSPECTOR GENERAL
U. S. DEPARTMENT OF AGRICULTURE

U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2021 Federal Information Security Modernization Act



Audit Report 50503-0005-12

October 2021

IMPORTANT NOTICE

This audit report contains sensitive information that has been redacted for 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 2021 Federal Information Security Modernization Act

Audit Report 50503-0005-12

As required by FISMA, OIG reviewed USDA's ongoing efforts to improve its information technology security program and practices during FY 2021.

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 2021. This audit covered three agencies operating 102 of the Department's 312 operational FISMA reportable systems.

RECOMMENDS

We recommend the Department: (1) retire or supersede IT security policies and procedures on the Department Directives website in a timely manner; and (2) use various communication mediums (e.g., The Federal Chief Information Security Officer Council, Information System Security Manager meetings, etc.) during the policy clearance process to inform employees, contractors, and other stakeholders of required practices and procedures; implement an effective patch or upgrade process for mobile device; capture mobile devices vulnerabilities in the Department's reporting system; address POA&Ms that are past their due date to ensure identified security weaknesses are remediated in a timely manner; and develop the processes for documenting and implementing lessons learned, among other recommendations.

WHAT OIG FOUND

The United States Department of Agriculture (USDA) continues to take positive steps to improve its information technology (IT) security posture, but many weaknesses remain. In FY 2018–2020, there were 10 open recommendations at the beginning of fiscal year (FY) 2021. During FY 2021, four recommendations were closed. We have also issued 16 new recommendations based on security weaknesses identified in FY 2021.

The Office of Management and Budget (OMB) 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. 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.

USDA OFFICE OF INSPECTOR GENERAL
United States Department of Agriculture

DATE: October 29, 2021

AUDIT NUMBER: 50503-0005-12

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 2021 Federal Information Security Modernization Act Audit

This report presents the results of the subject review. The instructions for fiscal year (FY) 2021 Federal Information Security Modernization Act are outlined in the FY 2021 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics, v1.1, dated May 12, 2021. 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 and the proposed corrective actions plans will be reviewed as part of the management decision process.

In accordance with Departmental Regulation 1720-1, final action needs to be taken within 1 year of each management decision to prevent being listed in the Department's annual Agency Financial Report. For agencies other than OCFO, please follow your internal agency procedures in forwarding final action correspondence to OCFO.

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.

United States Department of Agriculture
Federal Information Security Modernization Act of 2014
Audit Report for Fiscal Year 2021

RMA Associates
Auditors. Consultants. Advisors.

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

September 29, 2021

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 2021

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) 2021. The objective of this audit was to evaluate the effectiveness of the Department's information security program and practices for FY 2021. We conducted the audit in accordance with *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 2021 Inspector General FISMA Reporting Metrics Version 1.1* (May 12, 2021) 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.

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

Sincerely,

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 2021

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 the use of technology enables and enhances the sharing of information instantaneously among stakeholders, it can also allow an organization's networks and IT resources to be 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) 2021 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. One such area is increasing the maturity of the Federal Government's Supply Chain Risk Management (SCRM) practices. As noted in the Federal Acquisition Supply Chain Security Act of 2018, agencies are required to assess, avoid, mitigate, accept, or transfer supply chain risks. The *FY 2021 IG FISMA Reporting Metrics* included a new domain focused on SCRM within the Identify function. This new domain focuses on the maturity of agency SCRM strategies, policies and procedures, plans, and processes to ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and SCRM requirements. The new domain references SCRM criteria in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*. According to the Department of Homeland Security (DHS), in order to provide agencies with sufficient time to fully implement NIST SP 800-53, Revision 5, in accordance with Office of Management and Budget (OMB) A-130, these new metrics should not be considered for the purposes of the Identify framework function rating.[1]

Also, within the Identify function, specific metric questions have been reorganized and reworded to focus on the degree to which cyber risk management processes are integrated with enterprise risk management (ERM) processes. As an example, IGs are directed to evaluate how cybersecurity risk registers are used to communicate information at the information system, mission/business process, and organizational levels. These changes are consistent with NIST Interagency Report 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)*,

[1] Please note eight out of nine domains were subject to NIST SP 800-53 Revision 4 standards. The SCRM domain was subject to NIST SP 800-53 Revision 5 standards, but is not considered for the purpose of the Identify Function framework rating because of implementation timing concerns, as communicated to the FISMA community by DHS.

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

which provides guidance to help organizations improve the cybersecurity risk information they provide as inputs to their ERM program.[2]

Furthermore, OMB has issued guidance on improving vulnerability identification, management, and remediation. Specifically, Memorandum M-20-32, *Improving Vulnerability Identification, Management and Remediation*, September 2, 2020, provides guidance to Federal agencies on collaborating with members of the public to find and report vulnerabilities on Federal information systems. In addition, the DHS Binding Operational Directive 20-01, *Develop and Publish a Vulnerability Disclosure Policy*, September 2, 2020, provides guidance on the development and publishing of an agency's vulnerabilities disclosure policy and facilitates an agency's awareness of otherwise unknown vulnerabilities. The *FY 2021 IG FISMA Reporting Metrics* included a new question (#24) to measure the extent to which agencies utilize a vulnerability disclosure policy as part of agencies' vulnerability management program for internet-accessible Federal systems.

In addition, the IG metric questions related to the implementation of policies and procedures have been reorganized and streamlined to reduce duplication and redundancies.

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.

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 provide 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 DHS.[3]

[2] National Institute of Standards and Technology Interagency Report 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)*, Oct. 2020.
[3] 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.

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

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.[4]

FISMA "directs the Secretary to consult with and consider guidance developed by NIST to ensure that operational directives do not conflict with NIST information security standards."[5]

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.[6]

Further, FISMA "requires OMB to ensure the development of guidance for evaluating the effectiveness of information security programs and practices."[7] As part of NIST's statutory role in providing technical guidance to Federal agencies, NIST works with agencies in developing information security standards and guidelines. NIST developed an integrated Risk Management Framework that effectively coordinated 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:[8]

- 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

[4] Ibid.
[5] Ibid.
[6] Ibid.
[7] Ibid.
[8] Ibid.

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

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.[9]

FISMA Reporting Metrics

The *FY 2021 IG FISMA Reporting Metrics*[10] 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 and other stakeholders. The FY 2021 metrics represent a continuation of work begun in FY 2016 when the IG metrics[11] 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. Also, this year, a new SCRM domain was added within the Identify function area. According to DHS, in order to provide agencies with sufficient time to implement NIST SP 800-53 Revision 5, the SCRM domain was not considered in the calculation of the Identify function rating.

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:

[9] NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Apr. 2013.
NIST SP 800-53 Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, Sep. 2020.
[10] *FY 2021 IG FISMA Reporting Metrics v1.1* May 2021.
[11] *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

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 2021 IG FISMA Reporting Metrics* states 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 assigns points to agencies based on their achievement of various levels of maturity. Ratings throughout the nine 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 there are seven questions 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 nine domains:

- **Identify**, which includes questions pertaining to risk management and supply chain 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.

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

The answers to the 66 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 2021 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 2021 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 2021 FISMA testing.

USDA is a large, complex organization and includes 34 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 the Department'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 the Department'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 the Department's overall security posture.

One of the Department's strategic goals is to ensure USDA 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.[12]

[12] 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

The Department's overall maturity level remained at Level 3: "Consistently Implemented." At Level 3, policies, procedures, and strategies are formalized and documented, and they are consistently implemented. 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 its assessments. [13]

Due to the Department's maturity level of "Consistently Implemented," the security program for FY 2021 was not effective. Accordingly, 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 report.

The 66 FISMA Reporting Metrics are grouped into five functions and nine domains. For the FY 2021 FISMA, the maturity levels for the five functions are shown below:

Table 2: The Department's Maturity Levels

Function	Maturity Level	
Function 1: Identify		Consistently Implemented (Level 3)
• Risk Management	Consistently Implemented (Level 3)	
• Supply Chain Risk Management	Ad Hoc (Level 1)	
Function 2: Protect		Consistently Implemented (Level 3)
• Configuration Management	Consistently Implemented (Level 3)	
• Identity and Access Management	Consistently Implemented (Level 3)	
• Data Protection and Privacy	Defined (Level 2)	
• Security Training	Defined (Level 2)	
Function 3: Detect—Information Security Continuous Monitoring		Consistently Implemented (Level 3)
Function 4: Respond—Incident Response		Consistently Implemented (Level 3)
Function 5: Recover—Contingency Planning		Defined (Level 2)
Overall Maturity Level		**Consistently Implemented (Level 3)**
Overall Effectiveness		**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 allow individual agencies to manage these control activities.

USDA worked extensively in FY 2021 to improve IT security through the closure of weaknesses. The Department reduced the number of outstanding OIG prior year recommendations through the implementation of corrective actions. For FISMA audits conducted from 2018 through 2020, there were 10 open recommendations at the beginning of FY 2021. During FY 2021, four recommendations were closed (see Exhibit B). We acknowledge that OCIO made a concerted effort to close the outstanding recommendations.

[13] The Department maintained the maturity level of "Consistently Implemented" (Level 3), the same as prior year.

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

For FY 2021, RMA issued 16 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.

Exhibit A contains our responses to the OMB/DHS/CIGIE FY 2021 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 established a Risk Management program that operated at the "Consistently Implemented" maturity level, which is the same maturity level as last year.

Risk Management comprises a collection of activities focused on managing information system-related security risks, establishing a strategic vision, goals, and objectives; and developing, implementing, and operating the systems supporting the organization's core missions and business processes. IT security policies are the foundation of a Risk Management Program and the principal method through which the Department communicates its mission, strategic plan, goals, and objectives. IT security policies are the fundamental defense in safeguarding assets and defining operational expectations. The Department is responsible for designing IT security policies and procedures to fit its circumstances and building them as an integral part of its operations. The Department posts its authoritative IT security policies and procedures to its Directives website.[14]

The Department had a process to review policies and procedures to determine currency, accuracy, and relevancy. If content is outdated, the policy is slated to be retired or succeeded, however, policies were not being retired or superseded in a timely manner. We found 19 out of 26 (73%) IT security policies and procedures to be retired or superseded were still on the website for 20–28 months after the designation. Also, the Directives website was not updated to reflect the internally designated status.

Also, the Department's IT security policies and procedures were not revised when Federal requirements were changed, resulting in an increased risk that security practices are outdated, unclear, misunderstood, or improperly implemented. We found the IT security policies and procedures referred to superseded OMB guidance from 2016 and NIST guidance from 2007. Some of the Federal guidance was outdated by 36–164 months.

- **FY 2021 Recommendation 1**: We recommend the Department 1) retire or supersede IT security policies and procedures on the Department Directives website in a timely manner; and 2) use various communication mediums (e.g., The Federal Chief Information Security Officer Council, Information System Security Manager meetings, etc.) during the policy clearance process to inform employees, contractors, and other stakeholders of required

[14] Directives General Information | Office of the Chief Information Officer (usda.gov) establishes the policies, responsibilities, standards, and procedures for issuing and reviewing Departmental Directives.

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

practices and procedures.

- **FY 2021 Recommendation 2**: We recommend the Department update IT security policies and procedures on its Directives website to include the most current Federal guidance.

The Department administers security controls over mobile devices by a central Mobile Device Management system. Mobile devices often need additional protection because their nature generally places them at higher exposure to threats than other devices (for example, desktop and laptop devices that are only used within the Department's facilities and networks). Therefore, mobile devices should have up-to-date operating systems that provide the proper level of security. The Department did not have an effective process for keeping the operating systems up-to-date on mobile devices.

The Department monitored the security of its mobile devices; however, mobile device users were responsible for managing the updates of their applications and operating systems. The Department did not force or push out the security patches or application upgrades, which may result in improper information disclosure, manipulation, or theft. The vulnerabilities identified on mobile devices were not included in the Department's central management reporting of network vulnerabilities. In addition, these vulnerabilities were not recorded and managed as Plan of Action and Milestone (POA&M) in accordance with Departmental Regulation (DR).[15] By not including these vulnerabilities in its central management reporting process, the Department may not be able to effectively communicate its mobile device weaknesses to the appropriate stakeholders.

- **FY 2021 Recommendation 3:** We recommend the Department implement an effective patch or upgrade process for mobile devices to address security deficiencies.

- **FY 2021 Recommendation 4:** We recommend the Department capture mobile devices vulnerabilities in the Department's reporting system.

POA&Ms are an essential tool to assist management in identifying, prioritizing, and tracking remediation of known security weaknesses. The longer a POA&M item is outstanding, the longer the weakness is exposed, preventing the control from performing as intended. The Department managed POA&Ms to identify and track weaknesses at the enterprise level and track system-specific weaknesses at the system level. The Department utilized POA&Ms to address security weaknesses and prioritize remediation efforts. Although the Department made progress in closing delayed and open POA&Ms during FY 2021, more improvement is needed. The Department has a significant number of POA&M past their projected completion date. As of May 24, 2021, 223 of 859, approximately 26% of FISMA reportable POA&Ms were delayed because the Department has not enhanced its process to evaluate the adequacy of justifications provided to ensure the estimated completion dates were met. These delayed POA&Ms may

[15] DR 3565-003 *Plan of Action and Milestones Policy*, Sept. 25, 2013, https://www.ocio.usda.gov/document/departmental-regulation-3565-003.

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

result in controls not operating as intended, and a lack of visibility over the Department's information security program effectiveness.

- **FY 2021 Recommendation 5:** We recommend the Department address POA&Ms that are past their due date to ensure identified security weaknesses are remediated in a timely manner.

The Department needs to communicate and benefit from the lessons learned from previous practice and actual risk events. By examining adverse events and losses from the past and reviewing missed opportunities (including those missed due to a risk-averse mindset), the Department can improve the risk management model and organizational outcomes.

We found the Department lacked formal lessons learned processes for Risk Management and a majority of the FISMA domains, including Configuration Management, Data Protection and Privacy, Information Security Continuous Monitoring, and Incident Response. Without formal disciplined lesson learned processes, the Department may not capture information from previous practice, and actual risk events lose the opportunity of strengthening the Department's security posture.

- **FY 2021 Recommendation 6:** We recommend the Department develop the processes for documenting and implementing lessons learned to instruct its employees to record, analyze, and revise control activities on a cyclical basis to improve the Department's security posture.

There was one recommendation related to risk management that was closed during FY 2021.[16]

Supply Chain Risk Management (Identify)[17]

The Department established an SCRM program that operated at the "Ad Hoc" maturity level.

The Department established an SCRM Strategy in February 2021, which addressed risk appetite, tolerance, monitoring, and evaluating supply chain risks. Our testing noted USDA developed policies and procedures to confirm systems, vendors, services, and components were compliant with USDA requirements. USDA also developed a designated acquisition review process to evaluate supply chain-related risks.

We are not making a recommendation in this area because of the efforts the Department made in establishing the SCRM strategy, which provides a foundation for implementation of its SCRM program.

[16] Recommendation 1 from FISMA FY 2020 (Audit 50503-0003-12). See Exhibit B.
[17] According to DHS, in order to provide agencies with sufficient time to implement NIST SP 800-53 Revision 5, the SCRM domain was not included in the calculation of the effectiveness of controls or the maturity level of USDA's security program.

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

Configuration Management (Protect)

The Department established a Configuration Management program that operated at the "Consistently Implemented" maturity level, the same maturity level as last year.

Configuration management controls security features for all hardware and software components of an information system. The security controls comprise a collection of activities focused on reducing threats and vulnerabilities to maintain the integrity of software and hardware systems. The Department supports a complex information system infrastructure that presented challenges in reducing known vulnerabilities. These vulnerabilities are weaknesses that could be exploited by internal or external malicious sources that undermine integrity, confidentiality, and availability of system resources. The longer the vulnerabilities remain on a system, the higher the risk it will be exploited.

The Department did not have an effective process for remediating known vulnerabilities on IT devices connected to the internal network in a timely manner. Even though the Department has improved its quality of tracking network vulnerabilities, more effort is needed to remediate vulnerabilities of their systems. DR 3530-006, Scanning and Remediation of Configuration and Patch Vulnerabilities (June 2019), states that critical vulnerabilities must be corrected within 14 days. All vulnerabilities rated as high, moderate, or low risk will be remediated within 30 days. According to *FY 2021 IG FISMA Reporting Metrics, for* Metric # 21 to be Consistently Implemented, critical vulnerabilities must be patched within 30 days. Effective vulnerability management reduces the risk of successful harmful breaches and decreases the time and effort necessary to respond appropriately after a breach. However, we analyzed the vulnerabilities reports on the internal network generated on April 1, 2021, through the Department's Security Information and Event Management (SIEM) tools. The reports showed 3,796 critical and high vulnerabilities. We found a significant percentage of critical and high vulnerabilities that were not patched for more than two years, including default configurations, insecure configuration, Transport Layer Security[18] encryptions weaknesses, and unapplied patches (as shown in the table below).

Table 3: Aging of Vulnerabilities

Vulnerabilities[19]	2-5 Years	Over 5 Years
Critical and High	18%	16%

- **FY 2021 Recommendation 7:** We recommend the Department patch it's critical, high, moderate, and low vulnerabilities on the IT devices connected to the internal network based on the specified timeframe mentioned in DR 3530-006 *Scanning and Remediation of Configuration and Patch Vulnerabilities*.

[18] Transport Layer Security is a cryptographic protocol used to secure data sent over a network, such as internet traffic.
[19] IT devices were either placed in service with known vulnerabilities or the vulnerabilities were outstanding on the device for an extended amount of time. The aging was calculated by noting year the Common Vulnerabilities and Exposures was created and comparing the year to 2021.

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

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.

Identity and Access Management controls seek to ensure the right people and things have the right access to the right resources at the right time. The Department developed multiple policies[20] that comprise the identity and access management program in compliance with applicable NIST SP standards. Additionally, the Department adequately planned to implement personal identity verification (PIV) for non-privileged and privileged access, in accordance with Government standards.[21] The Department's overall PIV usage for non-privileged users was above the OMB threshold of 85 % and PIV usage was mandatory for privileged users and was compliant across the Department.

The maturity level of this domain was Consistently Implemented. Our control testing for this domain found no exceptions, and the controls were operating as intended. Therefore, we are not making a recommendation in this area.

Data Protection and Privacy (Protect)

The Department improved the maturity level of its Data Protection and Privacy program from last year as "Ad Hoc" to this year as "Defined."

The Department maintained an inventory of the collection and use of personally identifiable information (PII) through CSAM. The Department reviewed and removed unnecessary PII collection on a biannual basis and used CSAM and their privacy website for disseminating privacy policies and procedures. Also, the Department conducted and maintained the most recent Privacy Impact Assessments (PIAs)/ Privacy Threshold Analyses (PTAs)/System of Record Notices (SORNs) in CSAM, an internal system of record not available to the public. However, the Department did not publicly post the most current PIAs and SORNs on the Department's external website. Also, based on our examination, 190 of the 215 (88%) PIAs were not reviewed and revised in the required time frame. In addition, one of the selected mission areas tested did not perform an annual review of the PIAs, PTAs, and SORNs. The Chief Privacy Officer was hired during FY 2021 and their team was in the process of consolidating the PIAs and SORNs to make sure the most updated PIAs and SORNs are reflected on their external website.

[20] DR 3640-001, *Identity, Credential, and Access Management*, June 8, 2021, 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*, June 24, 2021, https://www.ocio.usda.gov/document/departmental-regulation-4620-002.

[21] 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.

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

- **FY 2021 Recommendation 8:** We recommend the Department develop and implement a process to ensure the most current PIAs and SORNs are available to the public. Additionally, the mission areas should review the PIAs, PTAs, and SORNs annually.

The PII Breach Notification and Incident Response Plan was drafted, but not approved. The Plan established a cross-functional Privacy Incident Response Team that reviews, approves, and participates in executing the PII Breach Notification and Incident Response Plan. The Plan defined the process to determine whether notice to oversight organizations or affected individuals is appropriate. The Plan also established the process to determine the extent of harm, embarrassment, inconvenience, or unfairness to affected individuals. The Department is a significant organization in size and scope, and has a very complex IT infrastructure. As such, the process to review, modify, approve, and distribute the PII Breach Notification and Incident Response Plan can take a significant amount of time. Additionally, the Department did not conduct table-top exercises to improve its Data Breach Response Plan.

- **FY 2021 Recommendation 9:** We recommend the Department approve the PII Breach Notification and Incident Response Plan and perform table-top exercises annually.

The Department did not develop and administer role-based privacy training for individuals with PII responsibilities or activities involving PII. From a population of 10 privileged users selected for examination, we determined none of the 10 users completed the role-based privacy training. In addition, all three mission areas selected did not identify individuals with responsibilities for PII. Without role-based privacy training, individuals responsible for system administration and privacy of the Department information systems may not maintain the knowledge required to perform their responsibilities. In addition, personnel may be performing tasks without proper training, thus potentially increasing the risk that the Department's privacy information could become compromised, leading to privacy breaches.

- **FY 2021 Recommendation 10:** We recommend the Department develop and administer role-based privacy training to personnel responsible for PII or activities involving PII.

There were two prior recommendations related to data protection and privacy that were closed during FY 2021.[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.

Security awareness strategy addresses the organizations' intentions to assess security risk, respond to risk, and monitor risk. The Department did not have an approved authorized strategy

[22] Recommendation 7 from FISMA FY 2018 (Audit 50501-0018-12); 8 from FISMA FY 2020 (Audit 50503-0003-12). See Exhibit B.

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

that defined its security awareness and training strategy for developing, implementing, and maintaining a security awareness and training program tailored to its mission and risk environment.

- **FY 2021 Recommendation 11:** We recommend the Department authorize and approve its Security Awareness and Training Strategy.

A successful IT security program consists of: (1) developing an IT security policy that reflects business needs tempered by known risks; (2) informing users of their IT security responsibilities, as documented in agency security policy and procedures; and (3) establishing processes for monitoring and reviewing the program. Security awareness and training should be focused on the organization's entire user population. Management should set the example for proper IT security behavior within an organization. A security awareness program should begin with an effort that can be deployed and implemented in various ways and is aimed at all levels of the organization, including senior and executive managers. The effectiveness of this effort will usually determine the effectiveness of the awareness and training program.

An awareness and training program is crucial as it is the vehicle for disseminating information that users, including managers, need to do their jobs. In the case of an IT security program, it is the vehicle to communicate security requirements across the enterprise.

The Department did not develop and administer role-based security training for individuals with significant security responsibilities. From a population of 10 privileged users selected for examination, we determined there were no records that the 10 users completed the role-based security training. In addition, all three agencies selected have not identified individuals with significant security responsibilities. The Department was in the process of developing a role-based security training program.

- **FY 2021 Recommendation 12:** We recommend the Department develop, administer, and maintain records of completing role-based security training for individuals with significant security responsibilities.

Information Security Continuous Monitoring (Detect)

The Department increased the maturity level of its ISCM program from last year as "Defined" to this year as "Consistently Implemented."

The Department established policy[23] and a strategic plan[24] for the ISCM strategy. In addition, the Department has various methods and tools implemented to capture ISCM metrics from the different programs that encompass the overall ISCM strategy (i.e., risk management, configuration management, incident management, and POA&M management), which are

[23] DR 3540-003, *Security Assessment and Authorization*, Aug. 12, 2014, https://www.ocio.usda.gov/document/departmental-regulation-3540-003.
[24] *USDA Information Security Continuous Monitoring Strategic Plan*, Version 1.9, Apr. 2017.

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

reported and consolidated at a high level to provide a real time snapshot of USDA's risk environment.

The maturity level of this domain was Consistently Implemented. Our control testing for this domain found no exceptions, and the controls were operating as intended. Additionally, the Department was still in the process of consolidating its ISCM policies and strategies to reflect its transition to ongoing control and system authorization and implementing additional continuous monitoring tools. Therefore, we are not making a recommendation in this area.

Incident Response (Respond)

The Department decreased the maturity level of its Incident Response program from last year as "Managed and Measurable" to this year as "Consistently Implemented."

The Department published Incident Response policies[25] and procedures[26] that established the Department-level incident response program, which outlined response steps to security events or incidents. The policies established the guidelines and facilitated implementation for the Department to respond to and report cybersecurity events. In addition, the Department monitored and analyzed network traffic entering and leaving the Department's network by using DHS' program[27] for intrusion detection/prevention capabilities.

The Department lacked a formal lessons learned process for its Incident Response. RMA has noted this weakness under Risk Management Area. Therefore, we are not issuing a new recommendation.

Contingency Planning (Recover)

The Department established a contingency planning program that operated at the "Defined" maturity level, the same maturity level as last year.

Information system contingency planning refers to a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of information systems, operations, and data after a disruption. Contingency planning generally includes one or more of the following approaches to restore disrupted services: (1) restoring information systems using alternate equipment; (2) performing some or all of the affected business process using alternate processing (manual) means (typically acceptable for only short-term disruptions); (3) recovering information systems operations at an alternate location (usually acceptable for only long-term

[25] DR 3505-005, *Cybersecurity Incident Management,* Nov. 30, 2018, https://www.ocio.usda.gov/document/departmental-regulation-3505-005.
[26] DM 3505-005, *Cybersecurity Incident Management Procedures*, Nov. 30, 2018, https://www.ocio.usda.gov/document/departmental-manual-3505-005.
[27] 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).

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

disruptions or those physically impacting the facility); and (4) implementing appropriate contingency planning controls based on the information system's security impact level.

The Department and its mission areas did not have a specific requirement to identify and monitor the individuals that require contingency training. Our testing noted the Department did not provide the contingency training or ensure that all the contingency personnel participated in the annual contingency plan test/exercise. From the Department and its mission areas' information system contingency plans that listed individuals assigned responsibilities for the Plan, we selected 20 key personnel for examination of training compliance. We found 13 of the 20 personnel (65%) did not have contingency training certificates and had not participated in the annual contingency test.

- **FY 2021 Recommendation 13:** We recommend the Department and its mission areas administer and document contingency training for individuals with contingency roles and responsibilities.

The purpose of the business impact analysis (BIA) is to identify and prioritize system components. This is accomplished by correlating them to the mission/business processes the system supports. BIA information is used to characterize the impact on the processes in the event systems are unavailable.

The Department defined a policy,[28] procedural manual,[29] and standard template[30] to implement the enterprise-wide business continuity/disaster recovery program. The Department identified, monitored, and communicated the lack of review of BIAs through CSAM. However, the Department did not notify those parties responsible for taking corrective action. Our testing noted the Department did not review its BIAs annually as defined in DR 3571-001. We found Departmental officials did not document in CSAM whether BIAs were completed. Specifically, 86 (28%) of the 312 operational FISMA reportable systems reported in CSAM, had not completed the BIAs.

- **FY 2021 Recommendation 14:** We recommend the Department perform a complete review of its system-level BIAs within the timeframe prescribed by DR 3571-001.

The Department has a policy that requires a contingency plan to be in place and annually updated for every major information system. However, the Department was not compliant with this policy. Without ensuring that the necessary planning documentation is maintained and updated consistently, the Department may not be able to access critical information and resources to perform mission-critical business functions in the event of an extended outage or disaster.

[28] DR 3571-001, *Information System Contingency Planning and Disaster Recovery Planning*, June 1, 2016, https://www.ocio.usda.gov/document/departmental-regulation-3571-001.
[29] *Contingency Plan Exercise Handbook*, Revision 2.1, June 2017.
[30] *Contingency Plan Template*, v1.5, June 2017.

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

Within 12 selected systems, we found 2 systems did not have contingency plans reviewed and updated in FY 2021.

- **FY 2021 Recommendation 15:** We recommend the Department update and approve the information system contingency plans to reflect current business processes, requirements, and Governmentwide security policy and guidance.

The Department defined processes for information system contingency plan testing and exercises and included, as applicable, notification procedures, recovery operations, restoration of normal procedures, coordination with other business areas/continuity plans, and table-top and functional exercises. However, the Department did not consistently test system contingency plans. As of June 6, 2021, we found 16 systems of 312 operational FISMA reported systems were not tested annually.

In the FY 2020 FISMA audit, RMA issued Recommendation 9, stating the Department should 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 are reviewed annually to ensure corrective actions can be initiated, as necessary.[31] The Office of the Chief Financial Officer, (OCFO) closed this recommendation on June 28, 2021. However, our testing, based on a August 5, 2021 CSAM report, noted all contingency plans were not tested annually, thus indicating that the weakness still exists. As a result, we recommend that OCIO work with OCFO to reopen this recommendation. The Department should provide OCFO evidence that the corrective action is appropriately designed and effectively implemented prior to closing a recommendation.

- **FY 2021 Recommendation 16:** We recommend that the Department work with OCFO to reopen this recommendation. The Department should provide OCFO evidence that the corrective action is appropriately designed and effectively implemented prior to closing this associated recommendation.

[31] Recommendation 9 from FISMA FY 2020 (Audit 50503-0003-12). See Exhibit B.

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 Department wide. In total, our FY 2021 FISMA audit work covered three agencies and OCIO:

- Rural Development;
- Risk Management Agency; and
- National Agriculture Statistics Service.

As of August 5, 2021, the selected agencies operated 102 of the Department's 312 operational FISMA reportable systems.[32]

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 2021 and consisted of testing the 66 FISMA Reporting Metrics issued by DHS.

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 and 5*, 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 nine domains by a simple majority of the maturity level competent scores for each question within the domain, in accordance with the *FY 2021 IG FISMA Reporting Metrics Version 1.1.*

For testing the operating effectiveness of the security controls, we exercised professional judgment in determining the number of items to select for testing and the method to be used to select items. We 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 conducted this audit in accordance with Generally Accepted Government Auditing Standards[33] 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.

[32] Certain controls were tested at the agency level and some controls were tested at the Department level.
[33] GAO Government Audit Standards (2018 Revision).

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

Abbreviations

BIA.....business impact analysis
CIGIE.....Council of the Inspectors General on Integrity and Efficiency
CIO.....Chief Information Officer
CSAM.....Cyber Security Assessment Management System
DHS.....Department of Homeland Security
DR.....Departmental regulation
ERM.....enterprise risk management
FIPS.....Federal Information Processing Standards
FISMA.....Federal Information Security Modernization Act of 2014
FY.....fiscal year
GAO.....Government Accountability Office
ICAM.....identity credential and access management
IG.....Inspector General
ISCM.....information security continuous monitoring
IT.....information technology
NIST.....National Institute of Standards and Technology
OCFO.....Office of the Chief Financial Officer
OCIO.....Office of the Chief Information Officer
OIG.....Office of Inspector General
OMB.....Office of Management and Budget
PIA.....privacy impact assessment
PII.....personally identifiable information
PIV.....personal identity verification
POA&M.....plan of action and milestones
PTA.....privacy threshold analysis
SCRM.....Supply Chain Risk Management
SIEM.....security information and event management
SORN.....System of Records Notice
SP.....special publication
TBD.....to be determined
USDA.....United States Department of Agriculture

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 2021 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 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*
- NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*
- NIST SP 800-40, Revision 3, *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 800-53 Revision 5, *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, Volume 1, Revision 1, *Guide for Mapping Types of Information, and Information Systems to Security Categories*
- NIST SP 800-61, Revision 2, *Computer Security Incident Handling Guide*
- NIST SP 800-63, *Digital Identity Guidelines*
- NIST SP 800-83, Revision 1, *Guide to Malware Prevention and Handling for Desktops and Laptops*
- 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*

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

- 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, Revision 1, *Workforce Framework for Cybersecurity* (*NICE Cybersecurity Workforce Framework*

OMB Policy Directives

- OMB Memorandum M-21-02, *Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements*
- OMB Memorandum M-20-32, *Improving Vulnerability Identification, Management, and Remediation*
- 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-17-26, *Reducing Burden for Federal Agencies by Rescinding and Modifying OMB Memoranda*
- OMB Circular No. A-130, *Managing Information as a Strategic Resource*

DHS

- FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.1 May 12, 2021
- DHS Binding Operational Directive 20-01, *Develop and Publish a Vulnerability Disclosure Policy*

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,” “Exhibit B,” and “Exhibit C,” are not being publicly released due to the sensitive security content.

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)