OFFICE OF INSPECTOR GENERAL
U. S. DEPARTMENT OF AGRICULTURE

U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2023 Federal Information Security Modernization Act

Audit Report 50503-0011-12

July 2023

IMPORTANT NOTICE

This report contains sensitive content. It is 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 2023 Federal Information Security Modernization Act

Audit Report 50503-0011-12

As required by FISMA, OIG reviewed USDA's ongoing efforts to improve its information technology security program and practices during FY 2023.

OBJECTIVE

The objective of this audit was to determine the effectiveness of USDA's information security program.

REVIEWED

We evaluated security controls in accordance with applicable legislation, standards and guidelines, presidential directives, OMB memorandums, and USDA policies and procedures. This included security controls at both the Department level and system level. Of the USDA's 302 systems, we conducted system-level testing for 11 USDA-operated and 4 contractor-operated information systems.

RECOMMENDS

USDA should establish or improve internal processes to ensure that authorizations to operate (ATO) do not expire. USDA also needs to better manage access to information systems to prevent users from gaining unauthorized access. USDA mission areas should ensure that their system security plans (SSPs) are current and relevant, and USDA should complete its annual security control assessment to ensure that risks are identified, monitored, or addressed. OCIO should also notify USDA of all incidents reported to United States – Computer Emergency Readiness Team (US-CERT). Finally, USDA should quickly fix any vulnerabilities.

WHAT OIG FOUND

The United States Department of Agriculture (USDA) has worked diligently to improve its security posture, but some weaknesses remain. Of the 23 prior year recommendations, 1 remains open; 4 were closed by management, but KPMG did not have sufficient time to test whether the recommendations were implemented effectively; 2 were closed by management, but testing identified deficiencies related to the recommendations; and the remaining 16 closed by management were validated by KPMG as effectively remediated.

The Office of Management and Budget (OMB) establishes standards for an effective level of security and considers level 4, "Managed and Measurable," to be sufficient. However, we found the Department's maturity level to be at level 3, "Consistently Implemented," which is ineffective according to OMB's criteria. The Department and its agencies must develop and implement an effective plan to mitigate security weaknesses identified in the prior fiscal year recommendations.

DATE: July 27, 2023

AUDIT NUMBER: **50503-0011-12**

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

ATTN: **Megen Davis**
Audit Liaison
Strategic Planning, E-Government and Audits

FROM: **Janet Sorensen**
Assistant Inspector General for Audit

JANET SORENSEN Digitally signed by JANET SORENSEN Date: 2023.07.27 14:14:25 -05'00'

SUBJECT: U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2023 Federal Information Security Modernization Act

The Office of Inspector General contracted with KPMG LLP, an independent certified public accounting firm, to conduct an audit in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). The objective of this performance audit was to determine the effectiveness of USDA's information security program. This report presents the results of the subject review. The instructions for the fiscal year (FY) 2023 review are outlined in the Inspector General Federal Information Security Modernization Act of 2014 and Office of Management and Budget (OMB) Memorandum M-23-03 reporting guidance for FISMA, dated December 2, 2022. This report contains responses to the questions contained in these instructions. The contract required that the audit be performed in accordance with Government Auditing Standards and OMB guidance.

In connection with the contract, we reviewed KPMG LLP's report and related documentation and inquired of its representatives. Our review, as differentiated from an audit in accordance with Government Auditing Standards, was not intended to enable us to express, and we do not express opinions on the effectiveness of USDA's information security program. KPMG LLP is responsible for the attached report, dated July 24, 2023, and the conclusions expressed in the report. However, our review disclosed no instances where KPMG LLP did not comply, in all material respects, with Government Auditing Standards and OMB guidance.

Your written response to the draft is included in its entirety at the end of the report. Corrective action plans for the recommendations contained in the report should be provided to the Office of Inspector General within 60 days of this report date.

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 (https://usdaoig.oversight.gov/) 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.

U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2023 Federal Information Security Modernization Act

July 24, 2023

kpmg.com

KPMG LLP
Suite 900
8350 Broad Street
McLean, VA 22102

Chief Information Officer and Inspector General
U.S. Department of Agriculture
1400 Independence Ave., SW
Washington, DC 20250

U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2023 Federal Information Security Modernization Act

This report presents the results of our independent performance audit of the United States (U.S.) Department of Agriculture's (USDA or Department) information security program and practices for its information systems. We conducted our performance audit from December 14, 2022, through July 14, 2023, and our results are through the period of October 1, 2022, through June 30, 2023.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). Those standards require that we plan and perform the performance audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our performance audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our performance audit objectives.

In addition to GAGAS, we conducted this performance audit in accordance with the Consulting Services Standards established by the American Institute of Certified Public Accountants (AICPA). This performance audit did not constitute an audit of financial statements or an attestation level report as defined under GAGAS and the AICPA standards for attestation engagements.

In accordance with the Federal Information Security Modernization Act of 2014 (FISMA), the objective of this performance audit was to determine the effectiveness of USDA's information security program. As such, we evaluated relevant security controls and processes referenced in the five Cybersecurity Framework Function (hereafter, Cybersecurity Function) areas outlined in the Office of Budget and Management's (OMB) *Fiscal Year (FY) 2023-2024 Inspector General (IG) Federal Information Security Modernization Act of 2014 Reporting Metrics* (FY 2023 IG FISMA Reporting Metrics), issued on February 10, 2023. We responded to the FY 2023 IG FISMA Reporting Metrics and assessed the maturity levels on behalf of the USDA Office of Inspector General (OIG). (See Appendix II: FY 2023 IG FISMA Reporting Metrics). As part of our testing, we also followed up on the status of prior year recommendations.[1]

[1] Audit Report 50503-0003-12, *Fiscal Year 2020 Federal Information Security Modernization Act*, Oct. 29, 2020; Audit Report 50503-0005-12, *Fiscal Year 2021 Federal Information Security Modernization Act*, Oct. 29, 2021; and, Audit Report 50503-0009-12, *Fiscal Year 2022 Federal Information Security Modernization Act*, Sept. 27, 2022.

Based on the maturity levels calculated in CyberScope,[2] we determined USDA's information security program was not effective as it did not fully adhere to applicable FISMA requirements, OMB policy and guidance, and the National Institute of Standards and Technology (NIST) standards and guidelines. According to FY 2023 IG FISMA Reporting Metrics, a security program is considered effective if the calculated average of the FY 2023 Core IG Metrics and supplemental metrics are at least Level 4 (Managed and Measurable). **Table 1** below depicts the maturity levels for the five Cybersecurity Functions we assessed for USDA's information security program. CyberScope calculates the ratings for the core and supplemental metrics separately.

Table 1: Maturity Levels for Cybersecurity Functions

Cybersecurity Functions & FISMA Metric Domain Areas	Assessed Maturity Level for USDA's Information Security Program
1. Identify Risk Management (RM) Supply Chain Risk Management (SCRM)	*1. Level 3: Consistently Implemented* RM – Level 3 SCRM – Level 3
2. Protect Configuration Management (CM) Identity and Access Management (IAM) Data Protection and Privacy (DPP) Security Training (ST)	*2. Level 3: Consistently Implemented* CM – Level 2 IAM – Level 4 DPP – Level 3 ST – Level 3
3. Detect Information Security Continuous Monitoring (ISCM)	*3. Level 3: Consistently Implemented* ISCM – Level 3
4. Respond Incident Response (IR)	*4. Level 4: Managed and Measurable* IR – Level 4
5. Recover Contingency Planning (CP)	*5. Level 3: Consistently Implemented* CP – Level 3
Overall Maturity Level	**Level 3: Consistently Implemented**
Overall Effectiveness	**Not Effective**

Source: CyberScope Appendix A: Scoring Maturity Model

During FY 2023, we tested security controls at the Department level and for 15 USDA systems, 11 of which were USDA operated and 4 contractor operated. We identified and reported six new findings (see the section of this report titled Audit Recommendations and Findings) specific to the FY 2023 IG FISMA Reporting Metrics. The findings were identified in four of the five FISMA Cybersecurity Functions (Identify, Protect, Detect, and Respond) and in five of the nine FISMA Metric Domains (RM, CM, IAM, ISCM, and IR).

[2] CyberScope, operated by Department of Homeland Security (DHS) on behalf of OMB, is a web-based application designed to streamline Information Technology (IT) security reporting for Federal agencies. It gathers and standardizes data from Federal agencies to support FISMA compliance. In addition, IGs provide an independent assessment of effectiveness of an agency's information security program. USDA OIG must report its assessment results to DHS and OMB annually through CyberScope.

We identified findings associated with the following: (1) information systems that were operating with expired authorizations to operate (ATO); (2) account management controls that were not operating effectively because account reviews and reauthorizations were not completed, evidence of account authorization was not maintained, and inappropriate access was granted; (3) system security plans (SSP) did not comply with required information security policies; (4) security control assessments were incomplete; (5) the OIG was not notified of incidents reported to United States Computer Emergency Readiness Team (US-CERT); and (6) vulnerabilities were not remediated in a timely manner. We made 22 recommendations related to these findings that, when implemented, should strengthen USDA's information security program if effectively addressed by management.

We also evaluated the implementation of recommendations identified during the FY 2020, FY 2021, and FY 2022 FISMA performance audits, during our period of performance that ended on July 14, 2023. We determined:

- 1 of 23 recommendations remained open.
- 4 recommendations were closed by management, but KPMG did not have sufficient time to test whether the recommendations were implemented effectively.
- 2 recommendations were closed by management but testing by KPMG identified deficiencies related to the recommendations.
- 16 recommendations were closed by management and validated by KPMG as effectively remediated were assigned a status of "Closed." (See Appendix III: Status of Prior Recommendations).

We caution that projecting the results of our performance audit to future periods is subject to the risks that controls may become inadequate because of changes in conditions or because compliance with controls may deteriorate.

This report is intended solely for the use of USDA, USDA OIG, DHS, Government Accountability Office, and OMB and is not intended to be and should not be relied upon by anyone other than these specified parties.

KPMG LLP

July 24, 2023

Table of Contents

Background

KPMG LLP (KPMG) performed the fiscal year (FY) 2023 independent Federal Information Security Management Act of 2014 (FISMA) audit, under contract with the United States Department of Agriculture (USDA or Department) and on behalf of USDA Office of Inspector General (OIG), as a performance audit in accordance with Generally Accepted Government Auditing Standard (GAGAS). USDA OIG monitored our work to ensure that we met professional standards and contractual requirements.

USDA relies extensively on information technology (IT) systems and resources to accomplish its mission. The IT systems and resources strengthen management and oversight of the Department's procurement, property, and finances to help 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 ability to share information instantaneously among stakeholders through computers and networks, it also makes an organization's networks and IT resources vulnerable to malicious activity and exploitation by internal and external sources. Insiders with malicious intent, recreational and institutional hackers, and attacks by foreign intelligence organizations are significant threats to the Department's critical systems.

Agency Overview

USDA's mission is to provide effective, innovative, science-based public policy leadership in agriculture, food and nutrition, natural resource protection and management, rural development, and related issues with a commitment to delivering equitable and climate-smart opportunities.

USDA has established six strategic goals in support of its mission:[3]

1. *Combat Climate Change to Support America's Working Lands, Natural Resources, and Communities*: The Department must lead with investments in science, research, and climate-smart solutions. These investments will mitigate the impacts of climate change, increase adaptation to climate change, generate new income opportunities, and build generational wealth in disadvantaged communities.

2. *Ensure America's Agricultural System is Equitable, Resilient, and Prosperous*: USDA will safeguard animal and plant health, support farmers and ranchers' ability to start and maintain profitable cooperatives and businesses, and offer financial support to all producers affected by natural disasters. Additionally, USDA's research agencies will continue to introduce high-performance plants and animals and offer integrated management options to increase the efficiency of farming practices.

3. *Foster an Equitable and Competitive Marketplace for All Agricultural Producers*: USDA continues its efforts to promote American agricultural products and exports through promotion activities, development of international standards, removal of trade barriers by

[3] USDA Strategic Plan Fiscal Years 2022-2026 (Mar. 2022).

monitoring and enforcing existing trade agreements, and negotiation of trade agreements that benefit the U.S. agricultural economy. USDA will also work with developing countries to grow their economies and facilitate trade, developing markets of the future for all our producers.

4. *Provide All Americans Safe, Nutritious Food:* The Department continues to enhance its food inspection system with the goal of reducing illnesses from meat, poultry, and egg products and drive compliance with food safety regulations. At the same time, USDA's research, education, and extension programs will continue to provide science, information, tools, and technologies to reduce the incidence of foodborne illness. USDA will continue to develop partnerships that support best practices in implementing effective programs to ensure that eligible populations have access to programs that support their nutrition needs.

5. *Expand Opportunities for Economic Development and Improve Quality of Life in Rural and Tribal Communities*: USDA is taking bold action to promote rural prosperity and economic development by providing technical assistance and financing investments in rural water, electric, broadband, housing, community facilities, local and regional food systems, and rural businesses and cooperatives. USDA will leverage funds, stimulate private-public partnerships, and collaborate with communities to increase economic opportunities in underserved communities and build rural infrastructure. This includes working with Federal partners and various stakeholder groups to help rural and Tribal communities thrive.

6. *Attract, Inspire, and Retain an Engaged and Motivated Workforce that's Proud to Represent USDA*: In the coming years, USDA will build on best practices for a hybrid work environment and continue to evaluate the future of work at USDA. As such, USDA is committed to being a learning organization that tolerates risk-taking, explores the untested and unknown, and nurtures innovative ideas at all levels of the organization. USDA will prioritize learning and training throughout the employee experience at USDA.

Program Overview

USDA's Office of the Chief Information Officer (OCIO) operates within the Office of Secretary and has a mission of serving the information needs for USDA. OCIO supports the achievements of USDA's diverse mission areas by offering agile, world-class technology solutions to its stakeholders and applying innovative approaches to recruiting and developing a highly skilled workforce. OCIO develops, delivers, and defends the business information technologies that empower every aspect of USDA's mission.

In support of OCIO's mission, services related to end-user support, data center operations, application development, and wide-area network telecommunications are provided to USDA agencies and staff offices by the following five service centers, all of which fall under the purview of OCIO: Information Security Center (ISC), Digital Infrastructure Services Center (DISC), Enterprise Geospatial Management Office, Client Experience Center (CEC), and Information Resource Management Center.

Federal Information Security Modernization Act of 2014

On December 17, 2002, the President signed FISMA into law as part of the E-Government Act of 2002 (Public Law 107-347, Title III). The purpose of this act was to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets and provide a mechanism for improved oversight of Federal agency information security programs. FISMA was amended on December 18, 2014 (Public Law 113-283). The amendment (1) included the reestablishment of the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices, and (2) set forth the authority for the Secretary of the Department of Homeland Security (DHS) to administer the implementation of such policies and practices for information systems. FISMA requires that senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including assessing the risks and magnitude of the harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems.

Changes to IG FISMA Reporting Metrics for FY 2023

For FY 2023, the Council of the Inspectors General on Integrity and Efficiency (CIGIE), in coordination with OMB, DHS, the Federal Chief Information Officers, and the Chief Information Security Officer (CISO) Council, developed the FY 2023 Inspector General (IG) FISMA Reporting Metrics[4] for five Cybersecurity Functions[5] outlined in the National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework)*: Identify, Protect, Detect, Respond, and Recover.[6]

The FY 2023 IG FISMA Reporting Metrics represent a transition to a multi-year cycle to where core metrics are tested on an annual basis and the remaining supplemental metrics are tested every other year. The core metrics align to the Administration's priorities and requirements in Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*, as well as OMB guidance provided to agencies to further the modernization of Federal cybersecurity. Subsequently, OMB provided the following guidance: *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (M-22-09), *Multifactor Authentication and Encryption* (EO 14028), *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*

[4] OMB's *FY 2023-2024 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*, Feb. 10, 2023.

[5] In its *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, NIST created functions to organize basic cybersecurity activities at their highest level. These functions are Identify, Protect, Detect, Respond, and Recover. They aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities.

[6] The President issued EO 13636, *Improving Critical Infrastructure Cybersecurity*, on February 12, 2013, which established that "[i]t is the Policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties." In enacting this policy, the EO calls for the development of a voluntary risk-based Cybersecurity Framework—a set of industry standards and leading practices to help organizations manage cybersecurity risks. The resulting framework, created through collaboration between the Government and the private sector, uses a common language to address and cost-effectively manage cybersecurity risk based on business needs without placing additional regulatory requirements on businesses.

(M-21-31), *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response* (M-22-01), and *Software Supply Chain Security and Critical Software* (Section 4 of EO 14028).

In addition, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements* (M-23-03), highlights the continued focus of meeting goals of EO 14028 and M-22-09 by FY 2024.

The FY 2023 IG FISMA Metrics use the CIGIE maturity models for the nine FISMA Metric Domains:

- Risk Management (RM)
- Supply Chain Risk Management (SCRM)
- Configuration Management (CM)
- Identity and Access Management (IAM)
- Data Protection and Privacy (DPP)
- Security Training (ST)
- Information Security Continuous Monitoring (ISCM)
- Incident Response (IR)
- Contingency Planning (CP).

IG FISMA Reporting Metrics Scoring

The maturity model has five levels: Level 1: Ad hoc; Level 2: Defined; Level 3: Consistently Implemented; Level 4: Managed and Measurable; and Level 5: Optimized. **Table 2** details the five maturity levels to assess the agency's information security program for each Cybersecurity Function. A security program is considered effective if the calculated average of the metrics in a particular domain is Level 4 or higher. This is change from the prior year where the mode was used to make this determination and different questions were weighted differently. In addition, the core and supplemental metrics will be scored separately.

Table 2: Inspector General Assessed Maturity Levels

Maturity Level	Description
Level 1: Ad hoc	Policies, procedures, and strategy are not formalized; activities are performed in an ad hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategy are formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategy 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 strategy are collected across the organization and used to assess them and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

The ratings of the nine Metric Domains (RM, SCRM, CM, IAM, DPP, ST, ISCM, IR, and CP) were determined by a calculated average of the maturity levels entered for each metric question. When the assessed maturity levels were entered, the calculations were performed by CyberScope, which determined the rating for the Domains, Functions, and overall rating of USDA's information security program.

Objective, Scope, and Methodology

Objective

In accordance with FISMA,[7] the objective of this performance audit was to determine the effectiveness of USDA's information security program. As such, we assessed relevant security controls and processes referenced in the five Cybersecurity Function areas outlined within the FY 2023 IG FISMA Reporting Metrics. We reviewed corrective actions taken by USDA to implement the prior year FISMA performance audit recommendations. We also responded to the FY 2023 IG FISMA Reporting Metrics and assessed the maturity levels on behalf of USDA OIG.

Scope

To accomplish our objectives, we evaluated security controls in accordance with applicable legislation; FY 2023 IG FISMA Reporting Metrics; applicable NIST standards and guidelines, presidential directives, OMB memorandums referenced in the reporting metrics; and USDA policies and procedures. We performed procedures to assess whether selected controls established by USDA's information security program were suitably designed, implemented, and operating effectively from both an entity-wide and system-level perspective.

We performed testing at the entity level which included OCIO and the following service centers that are significant to this audit:

- ISC serves and supports USDA Agencies and Offices by helping to protect their mission-critical assets and information, thereby securing the country's diverse food, agriculture, rural and natural resources programs.

- DISC is responsible for the management and operation of the Data Center Hosting Services including the USDA Enterprise Data Centers in Kansas City, Missouri and Chicago, Illinois.

- CEC (formerly Client Technology Services) is a Federal government information-technology service provider that uses a business model to support the comprehensive IT requirements of Federal business. CEC provides comprehensive information technology, associated operations, security, and technical-support services to a customer base of more than 102,000 USDA end users located in more than 3,400 field, state, and headquarters offices across the U.S. and its territories, which include: Puerto Rico, Guam, U.S. Virgin Islands, Northern Mariana Islands, and Pacific Basin.[8]

[7]Federal Information Security Management Act of 2002 (FISMA), Pub. L. No.107-347, tit. III, Section 301, Subsection 3544(a)(1)(A), Dec. 17, 2002.
[8] www.usda.gov/ocio/centers.

We also selected 11 USDA-operated and 4 contractor-operated information systems out of 302 information systems that support USDA missions to perform system-level testing to determine if the security controls were implemented and operating as intended.

Methodology

We conducted this performance audit in accordance with GAGAS. Those standards require that we plan and perform the performance audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our performance audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our performance audit objective.

In addition to GAGAS, we conducted this performance audit in accordance with Consulting Services Standards established by the American Institute of Certified Public Accountants (AICPA). This performance audit did not constitute an audit of financial statements, or an attestation-level report as defined under GAGAS and the AICPA standards for attestation engagements.

We designed testing procedures for the purposes of assessing whether USDA controls were designed in accordance with relevant requirements and operated in a manner consistent with their intended design throughout the period under audit. When designing procedures to assess the operating effectiveness of manual controls, we applied non-statistical random selections where the sizes of the populations (i.e., the number of occurrences of the control) were the determining factor, as described in the following paragraphs. **Table 3** below provides the frequency of control operation (population size) and the minimum selection size and the following considerations:

Table 3: Minimum selection size based on frequency of control operation (population size)

Frequency of control operation (Size of the population)	Minimum selection size
Annual (1)	1
Quarterly (2–4)	2
Monthly (5–12)	2
Weekly (13–52)	5
Daily (53–365)	15
Recurring Manual (multiple times/day) (>365)	25

The following approach was agreed upon with USDA OIG for conducting this performance audit and determining the maturity levels for each of the five Cybersecurity Functions and nine FISMA Metric Domains from the FY 2023 Core and Supplemental IG Metrics:

- We requested OCIO management communicate its self-assessed maturity levels, where applicable, to confirm our understanding of the FISMA-related policies and procedures, guidance, structures, and processes established by USDA. The self-assessment helped us to plan our inquiries with management and understand the specific artifacts to evaluate as part of the FISMA performance audit.

- We performed test procedures over security controls referenced in the FY 2023 IG FISMA Reporting Metrics that system support teams performed to secure USDA information systems (where applicable), leveraging maturity Level 3 (Consistently Implemented) questions within the nine FY 2023 IG FISMA Reporting Metric Domains. If we identified findings associated with metrics that were tested in consideration of maturity Level 3 questions, we considered the nature of the identified finding(s) and assessed the maturity at Level 1 (Ad hoc) or Level 2 (Defined) for the questions with responses indicating control failures.

- For metrics determined to be at maturity Level 3, we performed further procedures leveraging maturity Level 4 (Managed and Measurable) questions within the nine IG FISMA Reporting Metric Domains. If we identified findings associated with metrics that were tested in consideration of maturity Level 4 questions, we assessed the maturity at Level 3 for the questions with responses indicating control failures.

- For metrics determined to be at maturity Level 4, we performed further procedures leveraging maturity Level 5 (Optimized) questions within the nine FY 2023 IG FISMA Reporting Metric Domains. We performed these procedures to evaluate the design of the metrics. If we identified findings associated with metrics that were tested in consideration of maturity Level 5 questions, we assessed the maturity at Level 4 for the questions with responses indicating control failures.

Per the results of our test procedures, we entered the assessed maturity level for each of the FY 2023 core and supplement metrics into the CyberScope reporting tool, which automatically calculated the ratings for Domains, Functions, and overall effectiveness of the information security program.

Our procedures included the following to assess the effectiveness of the information security program and practices of USDA:

- Inquiry of information system owners, Information System Security Officers, system administrators, and other relevant individuals to walk through each control process;
- An inspection of the information security practices and policies established by USDA;
- An inspection of the information security practices, policies, and procedures in use across USDA; and
- An inspection of artifacts to determine the design, implementation, and operating effectiveness of security controls at the program and system levels.

We performed our fieldwork from December 14, 2022, through June 30, 2023. Our testing was performed remotely through meetings, walkthroughs, and observations with representatives from USDA. During our performance audit, we met with the Department and the Mission Areas to discuss our findings.

Criteria

We focused our FISMA performance audit approach in consideration of Federal information security guidance developed by NIST and OMB. NIST special publications (SP) provide guidelines associated with the development and implementation of agencies' security programs. Federal agencies were required to update their security policies and procedures to comply with NIST SP 800-53, Revision (Rev.) 5, *Security and Privacy Controls for Information Systems and Organizations*.[9] We also leveraged a variety of USDA directives, manuals, standard operating procedures, and other system-level guidance for information security.[10] For each finding detailed in the Audit Findings and Recommendations section, we included the relevant USDA, OMB, and/or NIST criteria.

[9] NIST SP 800-53, Rev. 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, Sept. 2020.

[10] USDA Department-level directives, manuals, and other guidance for information security can be found via the USDA website at https://www.usda.gov/directives. Entity-wide and system-level specific policies and procedures are stored in restricted locations.

Overall Results

We assessed the effectiveness of USDA's information security program on a maturity model spectrum where the foundational levels indicate that sound policies and procedures are designed and developed and the advanced levels capture the extent to which those policies and procedures have been implemented and operating effectively. The overall maturity of USDA's information security program is then calculated based on the average rating of the associated domains. Based on the maturity levels calculated in CyberScope, USDA's information security program was not effective as it did not fully adhere to applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines. A security program is considered effective if the calculated average of the assessed maturity levels for the FY 2023 IG FISMA Reporting Metrics in CyberScope is determined to be Level 4: Managed and Measurable. **Table 4** below depicts USDA maturity levels for the five Cybersecurity Functions.

Table 4: Maturity Levels for Cybersecurity Functions

Cybersecurity Framework Functions & FISMA Metric Domain Areas	Maturity Level
1. Identify Risk Management (RM) Supply Chain Risk Management (SCRM)	*1. Level 3: Consistently Implemented* RM – Level 3 SCRM – Level 3
2. Protect Configuration Management (CM) Identity and Access Management (IAM) Data Protection and Privacy (DPP) Security Training (ST)	*2. Level 3: Consistently Implemented* CM – Level 2 IAM – Level 4 DPP – Level 3 ST – Level 3
3. Detect Information Security Continuous Monitoring (ISCM)	*3. Level 3: Consistently Implemented* ISCM – Level 3
4. Respond Incident Response (IR)	*4. Level 4: Managed and Measurable* IR – Level 4
5. Recover Contingency Planning (CP)	*5. Level 4: Managed and Measurable* CP – Level 3
Overall Maturity Level	**Level 3: Consistently Implemented**
Overall Effectiveness	**Not Effective**

Source: CyberScope Appendix A: Scoring Maturity Model

During FY 2023, we tested security controls referenced in the FY 2023 IG FISMA Reporting Metrics at the Department-level, at three OCIO service centers (ISC, DISC, and CEC) and for 15 information systems. We identified and reported six findings (see Audit Recommendations and Findings section). Findings were identified in three of the five FISMA Cybersecurity Functions (Identify, Protect, Detect, and Respond) and in five of the nine FISMA Metric Domains (RM, SCRM, ISCM, IAM, and IR). We also evaluated the implementation of recommendations from prior FISMA reports. Out of 23 previously open recommendations identified during the FY 2020, FY 2021, and FY 2022 performance audits, we determined:

- There was 1 recommendation that remained open.
- There were 4 recommendations closed by management, but KPMG did not have sufficient time to test whether the recommendation was implemented effectively.
- There were 2 recommendations closed by USDA, and KPMG identified that the issues recurred during the performance audit period.
- There were 16 recommendations successfully closed by USDA, and the issues did not recur during the performance audit period.

Audit Recommendations and Findings

Finding 1: Systems Operating with Expired Authorizations

KPMG identified 4 information systems that were operating with an expired authorization to operate (ATO). Specifically, the ATO for a contractor system expired on March 27, 2023, and continued to operate without a valid ATO. The ATO for another contractor system expired on February 10, 2023, but was re-authorized to operate on April 6, 2023. The ATO for a USDA system expired on March 27, 2023, and was retired from production on April 13, 2023. Finally, the ATO for another USDA system expired on February 26, 2023, and continued to operate without a valid ATO.

USDA Departmental Regulation (DR) 3540-003, *Security Assessment and Authorization*, August 12, 2014, requires all USDA IT programs, systems, contractor provided systems, including cloud systems and services, to have an ATO per the procedures outlined in the *Risk Management Framework (RMF) Process Guide* prior to being placed into operation. In addition, USDA Standard Operating Procedures for RMF, Step 5: *Authorize Information Systems*, version 1.1, May 2022, requires all activity of previously authorized systems in operation to be halted if, for whatever reason, an authorization is not issued.

Agency and program office representatives indicated resource constraints, lack of oversight and coordination, and difficulty finding contractor assistance with the assessment process prevented the timely completion of the security assessments prior to the ATOs expiring. As a result, there was insufficient time for the Authorizing Officials (AOs) to review the results of the assessments and re-authorize the systems.

In addition, OCIO management did not define, within its *RMF Process Guide*, the procedures, or circumstances by which agency and staff offices should request a temporary authorization, such as for a planned system retirement or disposal.

Failure to timely reauthorize information systems may result in a lack of established accountability for managing the information systems. This may lead to the management not fully understanding and responding to inherent and residual risks and the internal and external threats and vulnerabilities to the systems.

Recommendation 1 – OCIO management should improve internal processes so that internal ATO reviews are completed on time, prior to the existing ATOs expiring.

Recommendation 2 – OCIO management should improve oversight over contractors and enforce the timely completion of ATOs, in accordance with USDA policy.

Recommendation 3 – OCIO management should update existing policy and procedures to define the conditions under which temporary reauthorization decisions may be granted (i.e., systems scheduled for retirement and disposal).

Recommendation 4 – Rural Development management should improve system owner and support

staff communications with OCIO regarding system retirements and disposals to ensure their information systems remain authorized until system disposal is completed.

Finding 2: USDA Did Not Effectively Manage User Access to Systems

USDA's account management controls did not always operate effectively. We noted periodic account reviews were not consistently performed for an information system's privileged users to ensure access was appropriate. Specifically, we noted evidence of review for one of two quarters selected was not available. We noted evidence of access approval for one of five selected new privileged users was not documented or retained for an application. We noted access request forms for a cloud application were not consistently retained or appropriately approved for two of five new privileged users tested. Specifically, we noted an approved privileged user's access request form was not retained. The other privileged user's assigned system roles did not match the permissions requested, and the user's access was provisioned in the cloud application before the approval noted in the access request form. We noted application management was unable to provide a system-generated list of privileged users with account creation and reauthorization dates until the conclusion of our performance audit field-testing. As a result, we were unable to test the effectiveness of the application access provisioning and reauthorization processes for this system. Finally, we noted a system support team did not implement a formal process to periodically review privileged user activity audit logs for the system in accordance with USDA policies.

USDA DR 3505-003, *Access Control for Information and Information Systems* (July 17, 2019), requires agencies to develop, implement, and maintain agency processes and procedures aligned with this DR to manage access to USDA information and information systems. The procedures should include requirements to verify that requests to create, modify, disable, or delete information system accounts or access privileges receive formal authorization by the system owner, employee manager, or contracting officer's representative. The procedures should include verification that the information provided with each account access request (including modifications) is correct and accurate. The procedures should allow for the monitoring and periodic validation of accounts and privileges. Finally, the procedures should require the review of system audit records for indications of inappropriate usage and report findings to designated organizational officials, as specified in internal procedures.

Furthermore, Government Accountability Office (GAO) *Standards for Internal Control in the Federal Government*, dated September 2014, states:

> Documentation of the Internal Control System, 3.09, "Management develops and maintains documentation of its internal control system."
>
> Design of Appropriate Types of Control Activities, 10.03, "… Appropriate documentation of transactions and internal control: Management clearly documents internal control and all transactions and other significant events in a manner that allows the documentation to be readily available for examination."

The Mission Areas generally attributed the access issues to a lack of oversight by OCIO management to ensure the mission areas, agencies, program offices and system teams' effective

implementation of controls, as required by USDA DR 3505-003. For one system, the system management was not aware they had to perform and document reviews of privileged users. For two other systems, the system management teams did not monitor or enforce retention requirements for user access request forms. For the last system, system management indicated a reliance on the identity and access management tool resulting in the inability to provide system-generated evidence identifying whether privileged user access was modified or created during the test period.

There is an increased risk that unauthorized or otherwise inappropriate user access is granted to USDA information systems without timely detection by USDA management. Such access could be used to make changes that negatively affect the accuracy, integrity, and availability of the system and its data.

Recommendation 5 – OCIO management should design and implement a quality control process to validate that designated management are incorporating and complying with the requirements of DR 3505-003.

Recommendation 6 – OCIO management should design and implement a process to ensure access control documentation, such as application user listings with the required data elements (i.e., account creation and recertification dates), is retained to support its system of internal controls and operational needs as required by GAO standards.

Recommendation 7 – Food Safety and Inspection Service management should implement a standardized process to conduct and monitor reviews of privileged application accounts to ensure appropriate access rights.

Recommendation 8 – Food Safety and Inspection Service management should implement a standardized process for the system teams to conduct, monitor, and maintain user access request forms prior to granting system access.

Recommendation 9 – Research, Education, and Economics management should implement a standardized process for the system teams to conduct, monitor, and maintain user access request forms prior to granting system access.

Recommendation 10 – Rural Development management should implement a standardized process for the system teams to conduct, monitor, and maintain user access request forms prior to granting system access.

Finding 3: SSPs Did Not Fully Comply with Required Information Security Policies

We determined that System Security Plans (SSPs) for 4 of 11 systems selected for testing[11] were not completed properly and did not reflect the current system environment per USDA policy and the NIST SPs 800-18, 37, and 53. Specifically, four systems did not document the correct implementation statuses of their security controls. Additionally, in the interconnection security agreements section for three systems, management did not include all interfaces.

USDA Standard Operating Procedures for RMF, Step 5: *Authorize Information Systems*, version 1.1, May 2022, states:

> An [Interconnection Security Agreement (ISA)] is only required when the connecting components have different Authorizing Officials. It is important to note that these connections must still be clearly annotated within the SSP and in the Relationships Tab within Cyber Security Assessment and Management (CSAM). Be sure to include the interface characteristics for each FISMA boundary the systems connect to, whether the connection is formally documented with an ISA or informally when within the purview of the same Mission Area AO boundary.

NIST SP 800-37, Rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*,[12] states that agencies should "Document the controls for the system and environment of operation in security and privacy plans."

NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*,[13] states:

> 3.14 Minimum Security Controls
> The description should contain 1) the security control title; 2) how the security control is being implemented or planned to be implemented; 3) any scoping guidance that has been applied and what type of consideration; and 4) indicate if the security control is a common control and who is responsible for its implementation.
>
> 3.11 System Interconnection/Information Sharing
> It is important that system owners, information owners, and management obtain as much information as possible regarding vulnerabilities associated with system interconnections and information sharing. This is essential to selecting the appropriate controls required to mitigate those vulnerabilities.

[11] While 15 systems were selected for testing in FY 2023, 4 of the systems were contractor-operated systems and therefore not subject to the same testing procedures as the other 11 USDA-operated systems.
[12] NIST SP 800-37, Rev. 2, *Risk Management Framework for Information Systems and Organizations: A system Life Cycle Approach for Security and Privacy* (Dec. 2018).
[13] NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems* (Feb. 2006).

Due to a lack of management oversight, USDA management did not ensure its system environments were adequately considered and fully documented within security documentation. Specifically:

- The three system teams informed us the above discrepancies were due to changes in CSAM and the transition to NIST SP 800-53, rev. 5. The control applicability and inheritance considerations will not take effect until the next security assessment is completed.
- A system team indicated there is confusion as to which interfaces, external or internal, should be included in the SSP.
- A system team informed us technical difficulties prevented them from adding the interconnection to the SSP.

Without accurate implementation details for security controls and interconnections, USDA is at risk of operating components that do not meet the minimum-security control standards for their respective boundaries. In addition, there is an increased risk that controls are not implemented correctly, or a system is approved without USDA management fully understanding the controls in place to mitigate the risks to the system.

Recommendation 11 – OCIO management should implement a quality control process to validate whether SSPs adhere to USDA Standard Operating Procedures for the RMF and NIST SPs 800-18, 800-37, and 800-53 and accurately reflect the current system environment.

Recommendation 12 – OCIO management should implement a quality control process to validate whether system-level SSPs, such as those tested, accurately reflect implementation statuses of their security controls and/or include all interfaces.

Recommendation 13 – Farm Production and Conservation management should review and update its SSPs to accurately reflect implementation statuses of their security controls and/or include all interfaces.

Recommendation 14 – Rural Development management should review and update its SSPs to accurately reflect implementation statuses of their security controls and/or include all interfaces.

Recommendation 15 – Food, Nutrition, and Consumer Services management should review and update its SSPs to accurately reflect implementation statuses of their security controls and/or include all interfaces.

Finding 4: USDA's Annual Assessment of Security Controls Is Incomplete

For 5 of 15 USDA information systems selected, the required security controls (hybrid or fully applicable) were not completely tested during FY 2022, per USDA's continuous monitoring schedule. System management informed us they purposefully selected a subset of the required controls to test with approval from OCIO; however, evidence of such approval was not provided. Mission areas, agencies, and program office management was not always familiar with the annual

security control assessment requirements for information systems based on security baselines or designation as a high value asset (HVA).

USDA's *Seven-Step RMF Process Guide*[14] requires that for each system, a subset of controls must be tested on an annual basis. OCIO defines what controls must be tested during any given year through a Departmental memo. The USDA *Cybersecurity Risk Management Strategy*[15] defines the process that should be followed in the event a control cannot be satisfied or risk cannot be adequately reduced. In that instance, OCIO or the Mission Area should follow formally document the risk acceptance or document the risk as a Plan of Action and Milestones (POA&M).

There is a lack of oversight by OCIO management for ensuring mission areas, and agencies are completing security control assessments in a complete and timely manner. USDA's Governance, Risk, and Compliance tool, or CSAM, was recently upgraded from NIST 800-53, Rev. 4 to Rev. 5; as a result, certain controls that were previously not applicable are required. System management informed us that this change, which was implemented in a short period of time, has led to certain security and risk management processes not being fully compliant. Due to resource constraints and competing priorities, not all required security controls could be assessed during the year.

Without complete and up-to-date security control assessments, critical risks may not be identified, monitored, or mitigated. This could result in an increased risk to the confidentiality, integrity, and availability of USDA information systems and the data.

Recommendation 16 – OCIO management should implement an effective quality control process to monitor that security controls are tested and documented during the assessments within the established annual timelines.

Recommendation 17 – OCIO management should develop and implement an effective review process to ensure the required security controls are assessed in accordance with the information system's security baseline categorization (e.g., High, Moderate, or Low) and designation as a HVA, as applicable.

Recommendation 18 – OCIO management should implement an effective quality control process for reviewing security control assessment plans either on a risk-based rotation or as needed basis. Such reviews will ensure the test plans incorporate the required controls for each application's baseline.

Recommendation 19 – OCIO management should develop department-wide communication or training to ensure USDA stakeholders and system personnel understand the requirements for performing and overseeing security control assessments.

Recommendation 20 – OCIO management should ensure a formal risk waiver is procured when selected security controls cannot be tested during the annual assessment.

[14] USDA, *Seven-Step RMF Process Guide*, Rev. 4.0 (Sept. 2019).
[15] USDA, *Cybersecurity Risk Management Strategy*, Version 1.0 (June 2021).

Finding 5: Failure to Notify OIG Regarding all Incidents Reported to US-CERT

The USDA ISC Incident Response Plan (IRP), dated February 28, 2023, contradicts requirements within USDA Departmental Manual (DM) 3505-005, *Cybersecurity Incident Management Procedures*. Specifically, DM 3505-005 requires OIG to be notified of every incident that is reported to United States – Computer Emergency Readiness Team (US-CERT). However, the ISC IRP only requires criminal incidents to be reported to the OIG.[16]

OMB Memorandum 20-04, *Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements*[17], states:

> An agency must notify the appropriate Congressional committees and its OIG of a major incident no later than seven days after the date on which the agency determined that it has a reasonable basis to conclude that a major incident, including a breach constituting a major incident, has occurred.

OCIO management did not consistently monitor its incident response reporting requirements process to ensure alignment with USDA DM 3505-005. Early OIG notification of all cyber-events, whether suspected criminal or not, is critical to ensure the integrity of USDA's cyberinfrastructure. Failure to notify the OIG may result in specifically trained criminal investigations being unable to collect and analyze electronic evidence and cyber-evidence before it is lost, hinder USDA's relationship with a broad array of external law enforcement, and facilitate the dissemination of sensitive law or erroneous information to the media.

Recommendation 21 – OCIO management should update the USDA ISC IRP to be aligned with DM 3505-005 and OMB policy.

Finding 6: Failure to Remediate Vulnerabilities in a Timely Manner

As of March 2, 2023, OCIO identified 40,785 critical vulnerabilities[18] that were not remediated within the required 14 days. Further, OCIO identified 180,255 high vulnerabilities[19] that were not remediated within 30 days. These metrics are reported to executive leadership through the Enterprise Patch and Vulnerability Group Monthly Executive meeting; however, OCIO has not developed performance measure(s) over the effectiveness of USDA's ability to remediate vulnerabilities within a timely manner.

---

[16] OCIO management took immediate action to remediate part of the condition. As of May 19, 2023, all incidents reported to US-CERT were also being reported to OIG.

[17] OMB Memorandum 20-04, *Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements*, Section II: *Reporting to Congress and Inspectors General* (Nov. 19, 2019).

[18] 34,350 out of the 75,135 critical vulnerabilities identified were remediated within the 14-day timeframe.

[19] 138,671 out of the 318,926 high vulnerabilities identified were remediated within the 30-day timeframe.

USDA DR 3530-006, *Scanning and Remediation of Configuration and Patch Vulnerabilities*,[20] states:

> 5. POLICY
> o. All critical vulnerability findings will be remediated within 14 days or in the timeframe indicated by the USDA CISO or designated authority.
>
> p. All vulnerabilities rated as high, moderate, or low risk will be remediated within 30 days or have a 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.

Due to lack of resources and competing business priorities, USDA management informed us that it was unable to remediate vulnerabilities within the required timeframe defined by DR 3565-003.

By not remediating vulnerabilities in a timely manner, there is an increased risk that open vulnerabilities can be leveraged to compromise the confidentiality, integrity, and availability of the data residing within USDA's IT environment.

Recommendation 22 – OCIO management should develop and implement quantitative and qualitative performance measures over the timely remediation of critical and high vulnerabilities to hold the Department and mission areas accountable for remediating vulnerabilities.

[20] USDA Departmental Regulation 3530-006, *Scanning and Remediation of Configuration and Patch Vulnerabilities* (June 5, 2019).

Conclusion

USDA's information security program was not effective for the five Cybersecurity Functions and nine FISMA Metric Domains as because it did not fully adhere to applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines. We identified findings in four of five Cybersecurity Functions and five of nine FISMA Metric Domains based on the procedures we performed related to the 15 selected information systems reviewed, along with Department-wide testing procedures. Based on the CyberScope results, USDA's information security program was assessed as not effective because a majority of the FY 2023 IG FISMA Reporting Metrics were rated as Consistently Implemented (Level 3).

We issued 6 findings and made 22 recommendations related to these findings that should strengthen USDA's information security program if effectively addressed by management. The root causes that led to the findings identified as part of this performance audit may contribute to findings for other systems outside of the scope of this audit.

To improve the maturity of its information security program, USDA should consider applying these recommendations to its entire universe of systems. Further, USDA should implement robust monitoring capabilities to continually assess the security state of these systems to include a process to hold service centers accountable for identified compliance gaps.

In a written response, the Chief Information Officer generally concurred with our findings and recommendations. (See Appendix IV: Agency's Response to Audit Report).

Appendix I: Glossary of Terms

AICPA	American Institute of Certified Public Accountants
AO	Authorizing Official
ATO	Authorization to Operate
BIA	Business Impact Analysis
CEC	Client Experience Center
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CISO	Chief Information Security Officer
CM	Configuration Management
CP	Contingency Planning
CSAM	Cyber Security Assessment and Management
DHS	Department of Homeland Security
DISC	Digital Infrastructure Services Center
DM	Departmental Manual
DPP	Data Protection and Privacy
DR	Departmental Regulation
EO	Executive Order
FISMA	Federal Information Security Modernization Act of 2014
FY	fiscal year
GAGAS	Generally Accepted Government Auditing Standards
GAO	Government Accountability Office
HVA	High-Value Asset
IAM	Identity and Access Management
IG	Inspector General
IR	Incident Response
IRP	Incident Response Plan
ISA	Interconnection Security Agreement
ISC	Information Security Center
ISCM	Information Security Continuous Monitoring
IT	Information Technology
KPMG	KPMG, LLC
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PII	Personal Identifiable Information
POA&M	Plan of Action and Milestones
RM	Risk Management
RMF	Risk Management Framework
SCRM	Supply Chain Risk Management
SORN	System of Records Notice
SP	Special Publications

SSP	System Security Plan
ST	Security Training
U.S.	United States
US-CERT	United States Computer Emergency Readiness Team
USDA/Department	United States Department of Agriculture

The subsequent sections of the report are not being publicly released due to concerns about the risk of circumvention of law:

Appendix II—FY 2023 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics (pages 19–44); and
Appendix III—Status of Prior Recommendations (pages 45–48).

Appendix IV: 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: Janet Sorensen
Assistant Inspector General for Audit
Office of Inspector General

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

SUBJECT: Office of Inspector General Audit #50503-0011-12, Fiscal Year 2023 "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 2023 #50503-0011-12 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.

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

We look forward to receiving the final OIG report.

If additional information is needed, please contact Megen Davis, Director, Strategic Planning, E-Government and Audits, at (301) 504-4299 or via email at megen.davis@usda.gov.

cc: Ja'Nelle L. DeVore, CISO, OCIO
Barry Lipscombe, DCISO, OCIO
Maria Vlioras, Executive Assistant, CIO, OCIO
Brittany Smith, Executive Assistant, CISO, OCIO
Megen Davis, Director, Strategic Planning, E-Government and Audits, OCIO-IRMC
Mohammad Nikravesh, Audit Liaison Official, OCIO-IRMC
Alanna Watkins, Chief, Policy and Compliance Branch, OCIO-ISC
Cutina Mosley, IT Security Specialist, OCIO-ISC

Learn more about USDA OIG
Visit our website: **https://usdaoig.oversight.gov/**
Follow us on Twitter: @OIGUSDA

How to Report Suspected Wrongdoing in USDA Programs

Fraud, Waste, and Abuse
File complaint online: **https://usdaoig.oversight.gov/hotline**

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)