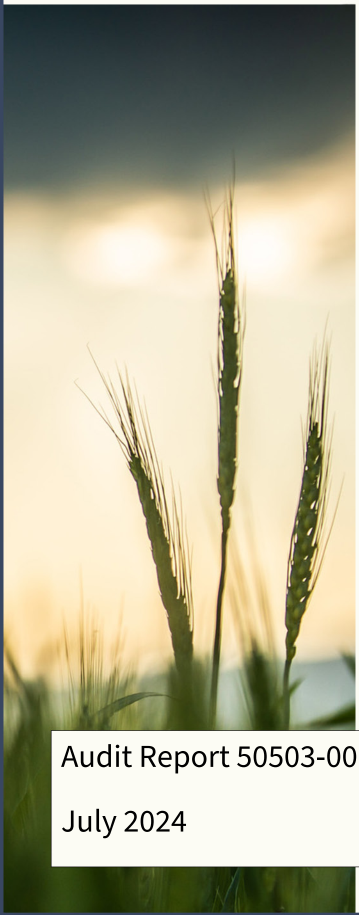
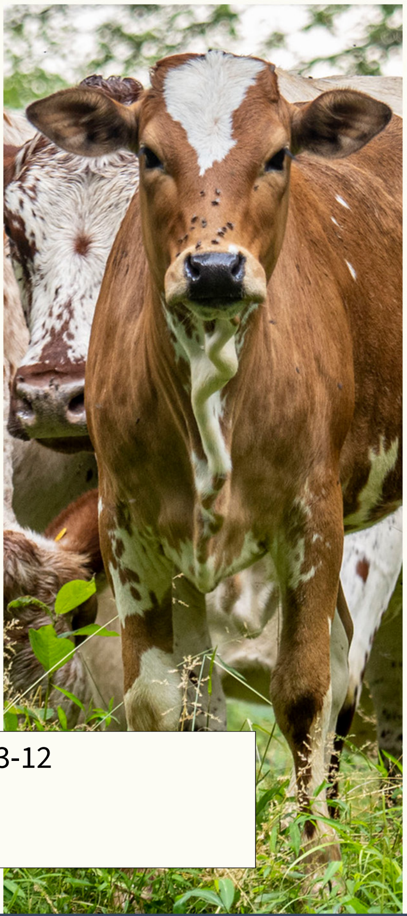
U.S. Department of Agriculture
Office of Inspector General

U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2024 Federal Information Security Modernization Act





Audit Report 50503-0013-12

July 2024

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 2024 Federal Information Security Modernization Act

Audit Report 50503-0013-12

As required by FISMA, OIG reviewed USDA's ongoing efforts to improve its information technology security program and practices during FY 2024.

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. Out of 328 information systems that support USDA missions, we selected 10 USDA-operated and 5 contractor-operated systems to perform system-level testing to determine if the security controls were implemented and operating as intended.

RECOMMENDS

We made 26 recommendations related to these findings that, when implemented, should strengthen USDA's information security program if effectively addressed by management. To improve the maturity of its information security program, USDA should consider applying these recommendations to its entire universe of systems.

WHAT OIG FOUND

The United States Department of Agriculture (USDA) has worked diligently to improve its security posture, with the core metric maturity average rising from the previous year. In addition, USDA closed 28 of 29 prior year recommendations; 1 recommendation remained open, 1 recommendation was partially implemented, and the remaining recommendations were successfully closed. Consistent with the Federal Information Security Modernization Act (FISMA) requirements, the Office of Management and Budget (OMB) policy and guidance, and the National Institute of Standards and Technology standards and guidance, USDA established and maintained its information security program and practices for the five Cybersecurity Functions and nine FISMA Metric Domains. USDA has increased its maturity level in one domain area to level 5, "Optimized." However, weaknesses still exist, and we made 26 new recommendations to address 12 identified deficiencies within USDA's information security program.

OMB establishes standards for an effective level of security and considers level 4, "Managed and Measurable," to be sufficient. However, we found USDA's maturity level to be at level 3, "Consistently Implemented," which is ineffective according to OMB's criteria. USDA should implement robust monitoring capabilities to continually assess the security state of its systems to include a process to hold service centers accountable for identified compliance gaps.

USDA

OFFICE OF INSPECTOR GENERAL

United States Department of Agriculture

DATE: July 25, 2024

AUDIT NUMBER: **50503-0013-12**

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

ATTN: **Angelo Rhodes**
Audit Liaison
Director of IT Policy and Audits (IRMC)

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

JANET SORENSEN
Digitally signed by JANET SORENSEN
Date: 2024.07.25 08:38:31 -05'00'

SUBJECT: U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2024 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) 2024 review are outlined in the Inspector General Federal Information Security Modernization Act of 2014 and Office of Management and Budget (OMB) Memorandum M-24-04 reporting guidance for FISMA, dated December 4, 2023. 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 9, 2024, 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 2024 Federal Information Security Modernization Act

July 9, 2024

kpmg.com

KPMG LLP
Suite 12000
1801 K Street, NW
Washington, DC 20006

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 2024 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) information security program and practices for its information systems. We conducted our performance audit from November 3, 2023 through May 31, 2024, and our results are through the period of October 1, 2023 through June 30, 2024.

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, the performance audit objectives were to:

1. Evaluate the effectiveness of the USDA's overall information technology (IT) security program by evaluating the five Cybersecurity Framework security functions outlined in the Office of Budget and Management's (OMB) Fiscal Year (FY) *2023-2024 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics* (FY 2024 IG FISMA Metrics):

   - 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.
   - Respond, which includes questions pertaining to Incident Response.
   - Recover, which includes questions pertaining to Contingency Planning.

2. Follow up on the status of corrective actions taken by the Office of the Chief Information Officer (OCIO) to implement the Office of Inspector General's (OIG) prior audit recommendations and determine whether corrective actions for open FISMA recommendations are effectively implemented for the corresponding FY 2024 IG Metric questions.[1]

As a result, we assessed USDA's information security program as Consistently Implemented (Level 3), which was ineffective according to OMB's FY 2024 IG FISMA Reporting Metrics guidance.

We made 26 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 2021, FY 2022 and FY 2023 FISMA performance audits, during our fieldwork testing period that ended on May 31, 2024. We determined that 1 of 29 recommendations remained open, 1 recommendation was partially implemented, and that 27 recommendations closed by management and validated by us 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, Department of Homeland Security (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 9, 2024

[1] Audit Report 50503-0005-12, *Fiscal Year 2021 Federal Information Security Modernization Act*, Oct. 29, 2021; Audit Report 50503-0009-12, *Fiscal Year 2022 Federal Information Security Modernization Act*, Sept. 27, 2022; and Audit Report 50503-0011-12, *Fiscal Year 2023 Federal Information Security Modernization Act*, July 28, 2023.

Table of Contents

Background

KPMG LLP (KPMG) performed the fiscal year (FY) 2024 independent Federal Information Security Management Act of 2014 (FISMA) audit, under contract with the United States Department of Agriculture (USDA 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 USDA'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 USDA. 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 USDA'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:[2]

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

[2] 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 four service centers, all of which fall under the purview of OCIO: Cybersecurity & Privacy Operations Center (CPOC), Digital Infrastructure Services Center (DISC), Client Experience Center (CEC), and Information Resource Management Center.

Federal Information Security Modernization Act of 2014

On December 17, 2002, the President signed FISMA[3] 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.

FY 2024 IG FISMA Reporting Metrics

OMB and the Council of the Inspectors General on Integrity and Efficiency (CIGIE), with review and feedback provided by several stakeholders, including the Federal Chief Information Officers (CIO) and Chief Information Security Officers councils, released OMB's guidance for implementing the requirements outlined in OMB Memorandum (M) 24-04, *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements,* outlined in the *FY 2023 – 2024 Inspector General FISMA Reporting Metrics*. The FY 2024 Inspector General FISMA Reporting Metrics are aligned with the five information security functions outlined in the *National Institute of Standards and Technology* (*NIST) Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework): Identify, Protect, Detect, Respond, and Recover. CIGIE maintained the maturity models for the following 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), and Contingency Planning (CP). **Table 1** illustrates the alignment of NIST Cybersecurity Framework to the FISMA Metric Domains within the FY 2024 IG FISMA Reporting Metrics.

[3] 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.

Table 1: Alignment of NIST Cybersecurity Framework to the FISMA Metric Domains

Cybersecurity Framework Functions	FISMA Metric Domains
Identify	Risk Management Supply Chain Risk Management
Protect	Configuration Management Identity and Access Management Data Protection and Privacy Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

Consistent with FY 2023, the models have five maturity levels: *Ad-hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized*. **Table 2** details the five maturity levels to assess the agency's information security program for each Cybersecurity Function.

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 *FY 2024 IG FISMA Reporting Metrics* represent a continuation of the work started in FY 2022, when the IG metrics reporting process was transitioned to a multi-year cycle. The FY 2024 IG FISMA Reporting Metrics included Core Metrics and Supplement Metrics Group 2, as depicted in **Table 3.**

Table 3: FY 2024 Metric Scoping

Core Metrics	Supplemental Metrics Group 2
1 - System Inventory	4 - Enterprise Architecture and System Categorization
2 - Hardware Inventory	6 - Information System Security Architecture
3 - Software Inventory	15 - SCRM Counterfeit Components
5 - Enterprise Risk Management & Risk Assessments	17 - CM Roles and Responsibilities
10 - RM Dashboards and Reporting	18 - Enterprise-Wide Configuration Management Policy
14 - SCRM Processes	23 - Application Configuration Change Control
20 - Configuration Settings	28 - Personnel Risk Designations
21 - Flaw Remediation	38 - Data Breach Response Plan
30 - MFA - General Users	39 - Privacy Awareness Training
31 - MFA - Privileged Users	44 - Cybersecurity Awareness Training
32 - Privileged User Account Management	45 - Specialized Security Training
36 - Encryption	50 - ISCM Performance Measures
37 - Data Exfiltration and Network Defenses	52 - Incident Response Policies and Procedures
42 - Workforce Assessment	53 - IR Roles and Responsibilities and Training
47 - ISCM Strategy	56 - Incident Response Reporting and Communication
49 - ISCM Processes	62 - Information System Contingency Plan
54 - Incident Response Tools and Detection	64 – Backups
55 - Incident Response Tools and Handling	
61 - Business Impact Analysis	
63 - ISCP Test, Training, and Exercise	

IG FISMA Reporting Metrics Scoring

According to the FY 2024 IG FISMA Reporting Metrics guidance, a security program is considered effective if the calculated average of the metrics in a particular domain is Managed and Measurable (Level 4) or higher. For FY 2024, a calculated average scoring model was used in which Core Metrics and Supplemental Metrics Group 2 were averaged independently to determine a domain's maturity calculation and provide data points for the assessed program and function effectiveness. The calculated averages of both the Core Metrics and Supplemental Metrics Group 2 are used as a data point to support the risk-based determination of overall program and function level effectiveness. Other data points considered include:

- The results of cybersecurity evaluations, including system security control reviews, vulnerability scanning, and penetration testing conducted during the review period;
- The progress made by agencies in addressing outstanding IG recommendations; and
- Reported security incidents reported during the review period.

IGs should use the CyberScope[4] reporting tool to calculate the maturity levels for each Cybersecurity Function and Domain and to submit the results of the IG Metrics evaluation. CyberScope provides supplementary fields to allow explanatory comments; IGs may use these fields to provide additional data supporting the Core Metrics evaluation results, and ultimately provide the overall effectiveness of the USDA's information security program.

[4] CyberScope, operated by DHS on behalf of OMB, is a web-based application designed to streamline information technology security reporting for federal agencies. It gathers and standardizes data from federal agencies to support FISMA compliance. In addition, Offices of Inspectors General provide an independent assessment of effectiveness of an agency's information security program. Offices of Inspectors General must also report their results to DHS and OMB annually through CyberScope.

Objective, Scope, and Methodology

Objective

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. Specifically, the performance audit objectives were to:

1. Evaluate the effectiveness of USDA's overall IT security program by evaluating the five Cybersecurity Framework security functions outlined in the FY 2024 IG FISMA Metrics:

    - 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.
    - Respond, which includes questions pertaining to Incident Response.
    - Recover, which includes questions pertaining to Contingency Planning.

2. Follow up on the status of corrective actions taken by the OCIO to implement OIG's prior audit recommendations and determine whether corrective actions for open FISMA recommendations are effectively implemented for the corresponding FY 2024 IG Metric questions.[5]

Scope

To accomplish our objectives, we evaluated security controls in accordance with applicable legislation; FY 2024 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:

- CPOC, formerly Information Security Center, 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.

[5] *Supra* note 1.

- CEC 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.[6]

We also selected 10 USDA-operated and 5 contractor-operated information systems out of 328 information systems that support USDA missions to perform system-level testing to determine if the security controls were implemented and operating as intended.

USDA's responsibilities as it relates to USDA-operated and contractor-operated systems differ. USDA's primary responsibilities with respect to contractor-operated systems are to monitor the effective information system controls of the systems and to help ensure the risk related to these systems did not exceed USDA's risk tolerance. Accordingly, the contractor-operated systems were subjected to a different set of audit procedures from the USDA-operated information systems.

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 4** below provides the frequency of control operation (population size) and the minimum selection size and the following considerations:

[6] www.usda.gov/ocio/centers.

Table 4: 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
Recurring Manual (multiple times/day) (>5000)[7]	45

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 Core Metrics and Supplemental Metrics Group 2:

- 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 2024 IG FISMA Reporting Metrics that system support teams performed to secure USDA information systems (where applicable), leveraging maturity Level 3 (Consistently Implemented) capabilities within the nine FY 2024 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) capabilities within the nine IG FISMA Reporting Metric Domains. If we identified findings associated with metrics that were tested in consideration of maturity Level 4, 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) capabilities within the nine FY 2024 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, we assessed the maturity at Level 4 for the questions with responses indicating control failures.

[7] Per Financial Audit Manual 450, if a recurring manual control has a population >5,000 then we must sample 45.

Per the results of our test procedures, we entered the assessed maturity level for each of the Core Metrics and Supplemental Metrics Group 2 into the CyberScope reporting tool, which automatically calculated the average core and supplemental ratings for Domains and Functions.

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 November 3, 2023, through May 31, 2024. Our testing was performed remotely through meetings, walkthroughs, and observations with representatives from USDA. During our performance audit, we met with OCIO 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, Release 5.1.1, *Security and Privacy Controls for Information Systems and Organizations*. We also leveraged a variety of USDA directives, manuals, standard operating procedures, and other system-level guidance for information security.[8] For each finding detailed in the Audit Findings and Recommendations section, we included the relevant USDA, OMB, and/or NIST criteria.

[8] 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

Consistent with the FISMA requirements, OMB policy and guidance, and NIST standards and guidance, USDA established and maintained its information security program and practices for the five Cybersecurity Functions and nine FISMA Metric Domains. In this report, we included 13 deficiencies noted within 4 of the 5 FISMA Cybersecurity Functions (Identify, Protect, Detect, and Recover) and in 7 of the 9 FISMA Metric Domains (RM, SCRM, CM, IAM, ST, ISCM, and CP). We made 26 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 from prior FISMA reports.[9] Out of 29 previously open recommendations identified during the FY 2021, FY 2022, and FY 2023 performance audits, we determined that 1 recommendation remained open, 1 recommendation was partially implemented, and that 27 recommendations were successfully closed by USDA and the issues did not recur during the performance audit period. One outstanding recommendation related to the IAM FISMA Metric Domain, and the other outstanding recommendation related to both RM and DPP Metric Domains.

As a result, we assessed USDA's information security program as Consistently Implemented (Level 3), which was ineffective according to OMB's FY 2024 IG FISMA Reporting Metrics guidance. **Table 5** below depicts USDA's maturity levels for the five Cybersecurity Functions.

Table 5: 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 2
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 3 DPP – Level 3 ST – Level 3
3. Detect Information Security Continuous Monitoring (ISCM)	*3. Level 4: Managed and Measurable* ISCM – Level 4
4. Respond Incident Response (IR)	*4. Level 5: Optimized* IR – Level 5
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

[9] *Supra* note 1.

Audit Recommendations and Findings

The following sections provide a summary of the audit recommendations and findings for each of the domains required to be monitored under FISMA. We did not identify any new recommended improvements for the DPP and IR FISMA Metric Domains and have, therefore, omitted them from this section.

Risk Management

The Risk management domain focuses on policies and actions that effectively manage information security risks within the organization. Federal agencies are required to consistently implement their security architecture across the enterprise, business process, and systems. The performance audit determined that USDA's risk management maturity level was Consistently Implemented (Level 3). To improve security in this domain, USDA should address the following issues:

Finding 1: Weaknesses with expired Interconnection Security Agreements and inaccurate entries

We determined that 2 of 10 USDA-operated systems selected for testing had expired Interconnection Security Agreements (ISAs) with external entities. These 2 systems collectively had 5 expired ISAs, with some of them expiring as far back as April 12, 2021, and the most recent one expiring on February 2, 2024. Both systems were systems owned by the Office of the Chief Financial Officer (OCFO) and authorized by the Departmental Administration Information Technology Office (DAITO). Additionally, we noted that 4 of the 5 expired ISAs were incorrectly listed as current within the Cyber Security and Assessment (CSAM).[10]

USDA guidance[11] stipulates that ISAs are required when there is a connection from a USDA system to an external system.

OCIO management attributed the issue to a lack of resource availability and budget constraints.

The purpose of an ISA is to establish a technical framework for agreed-upon security controls and define responsibilities for data shared between two systems. Without having finalized and mutually approved agreements, there is a risk that the terms of the agreements may not be fully understood or effectively implemented to address all security requirements. In addition, entering incorrect information in CSAM hindered USDA management from promptly identifying the backlog of Assessment and Authorization (A&A) activities within the OCIO's DAITO program office.

Recommendation 1 – We recommend Departmental Administration Information Technology Office management establish additional oversight controls to ensure interconnection security agreements are reviewed on an annual basis and signed every three years.

[10] CSAM is the application used by management to automate the system A&A process.

[11] USDA Standard Operating Procedures for Risk Management Framework (RMF), Step 5: Authorize Information Systems, version 1.1, May 2022.

Recommendation 2 – We recommend Departmental Administration Information Technology Office management establish a system of quality control to ensure the information entered in the assessment and authorization tool is accurate and reflective of a systems' actual control environment.

Finding 2: Weaknesses in the management of Plan of Action and Milestones (POA&M)

Plan of Actions and Milestones were not always documented and maintained in accordance with USDA policies and procedures. The following issues were identified for 2 of 10 USDA-operated systems selected for testing:

- 22 open POA&Ms have not been updated for periods ranging from 169 to over 1,313 days.
- 3 POA&Ms with a status of "Delayed" do not have a justification for the delay.

FISMA requires that agencies develop processes to remediate security weaknesses. OMB requires departments, like USDA, to develop POA&Ms for identified system weaknesses and to prioritize remediation based on the seriousness of each weakness.[12] According to USDA Departmental Regulation[13] (DR) 3565-003, *Plan of Action and Milestones Policy*, dated September 25, 2013, all POA&Ms are required to be entered into CSAM. If the status of the POA&M is "Delayed," a reason for the delay must also be selected.

DAITO management attributed this weakness to a lack of resource availability, budget constraints, and ongoing efforts to improve cybersecurity and overall security compliance for the DAITO authorized systems.

The failure to promptly complete corrective action plans to address existing weaknesses hinders DAITO management's ability to effectively manage, monitor, and evaluate processes established to ensure the ongoing effectiveness of its information system. Such actions could negatively affect the completeness, accuracy, and availability of a system and its data.

Recommendation 3 – We recommend Departmental Administration Information Technology Office management enforce the timely completion and update of all security artifacts, including Plan of Actions and Milestones.

Supply Chain Risk Management

The SCRM domain requires the development of policies, procedures, and programs to effectively manage supply chain risks associated with development, acquisition, maintenance, and disposal of systems. This includes monitoring third-party vendors and service providers and ensuring that appropriate contractual requirements, such as the prohibition of counterfeit components, are included in all contracts. We determined that USDA's supply chain risk management maturity

[12] OMB Circular A-130, *Managing Information as a Strategic Resource,* July 28, 2016.

[13] USDA DR 3565-003, *Plan of Action and Milestones Policy,* September 25, 2013.

level was Defined (Level 2). USDA can improve security in this domain by resolving the following issues:

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Configuration Management

The CM domain requires the development and implementation of standard configuration baselines that prevent or minimize exploitable system vulnerabilities in both software and hardware. In addition, CM policies and plans should be current with documented CM processes, and change requests documented, properly approved, and tested. We determined that USDA's CM maturity level was Defined (Level 2). USDA can improve security in this domain by resolving the following issue:

Finding 5: Vulnerabilities not promptly addressed

For one USDA-operated system, we determined the control to remediate vulnerabilities in accordance with DR was not operating effectively. During the annual security control assessment of this system, the security control assessor discovered that for one month, no vulnerabilities identified in the vulnerability scan reports were fixed or had a POA&M created. DAITO established a POA&M to monitor the fixing of the ineffective control.

The DR, states that all critical vulnerabilities are remediated within 14 days and all others will be remediated within 30 days or have POA&M created.

Delays in addressing system vulnerabilities and flaws creates opportunities for authorized and unauthorized users to exploit USDA's IT environments (operating systems, databases, and applications), leading to potential attacks, unauthorized modifications, and compromised data.

DAITO management attributed the deficiency to delays in completing cybersecurity upgrades. Furthermore, they stated that the system in question had recently undergone the necessary upgrades in September 2023 and intended to immediately request the closure of the POA&M but could not provide supporting documentation. Furthermore, since DAITO management is not actively monitoring their POA&Ms, they were unaware the POA&M was still open despite the issue having been corrected.

Recommendation 10 - We recommend Departmental Administration Information Technology Office management promptly address system vulnerabilities in accordance with Departmental Directive 3530-006.

Identity and Access Management

Proper identity and access management ensures that users and devices are properly authorized and authenticated to access information and information systems. In addition, policy and procedures must be in place for the creation, provisioning, maintenance, and eventual termination of accounts. We determined that USDA's identity and access management maturity level was Consistently

Implemented (Level 3). USDA can improve security in this domain by resolving the following issues:

Finding 6: Multi-factor user authentication not implemented for all systems

For 1 of 10 USDA-operated systems selected for testing, USDA needs to enforce the use of a Personal Identity Verification (PIV) or an equivalent multi-factor authentication (MFA) method for non-privileged users. Although the system does support MFA, and most users authenticate through USDA's electronic Authentication system using their PIV[17] as a primary means, there is a subset of non-privileged users that are still allowed to access the application with a username and password. Currently, 90 out of 11,611 USDA non-privileged users authenticate with a username and password as their primary and only means to access the system. Additionally, the current password-based authentication does not employ a list of commonly used, expected, or compromised passwords.

DR 3640-001, Identity, Credential, and Access Management, June 8, 2021, requires all federal employees and contractors to utilize MFA-compliant credentials, as outlined in Homeland Security Presidential Directive (i.e., HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors. The following examples represent USDA-approved compliant credentials:

- PIV credential;
- PIV-Interoperable credential; and
- Derived PIV per Office of Personnel Management requirements.

DAITO management provided several reasons for not requiring the use of MFA:

[redacted]

2. There are few MFA solutions that integrate well with the underlying software for which the selected system runs on. This lack of integration has prevented DAITO management from efficiently and quickly implementing MFA.
3. DAITO management recently attempted to require MFA through implementation of the software tool. However, due to a lack of oversight and planning, the vendor no longer supported integration, and a new solution has yet to be identified.

[17] USDA refers to its PIV credential that authorizes physical access to USDA facilities and information systems as a "LincPass."

[redacted]

Failure to implement strong authentication mechanisms increases the risk of unauthorized access to user accounts, thereby compromising the security of the organization's systems.

Recommendation 11 – We recommend Departmental Administration Information Technology Office management enforce multi-factor authentication, or the equivalent thereof, to the application.

Finding 7: Account management controls were not always followed

For 2 of 10 USDA-operated systems selected for testing, privileged access reviews were not performed in a timely basis. [redacted] management did not recertify the FY 2024 Quarter 1 access review of its privileged user accounts and groups until the Quarter 2 review. The DAITO performs monthly privileged access reviews delegated to seven different security coordinators who are responsible managing users under their purview. Each security coordinator is required to review their users and respond to the request affirming the review was completed. Between October 2023 and March 2024, we determined 17 of the 42 of the reviews were not confirmed as completed.

According to USDA DR 3505-003, *Access Control for Information and information Systems*, July 17, 2019, privileged user accounts and groups are required to be reviewed at least every quarter. Failure to perform these reviews puts the information system at risk of privileged users inappropriately retaining their access when no longer needed. This could lead to unauthorized modification and use of highly sensitive information stored in the system, as well as the potential for system failure due to unauthorized changes.

[redacted] management acknowledged this was an oversight that has already been self-identified and is being tracked for remediation. Management indicated this occurred due to the system's recent designation as a high value asset (HVA). While Federal requirements over HVA's have long been in place, USDA only recently published DR 3575-004, Information Technology Security Baselines and Security Control Tailoring, on November 21, 2023. The regulation is required to be implemented by all mission areas within 6 months after issuance prompting mission areas to implement the new requirements. The designation resulted in temporary reassignment of all available resources to fulfill the additional requirements for an HVA, impacting the timely completion of routine tasks, including the quarterly review of privileged users' access, which was temporarily halted.

DAITO management informed us that the current process lacks procedures to monitor and ensure the timely completion of privileged user access reviews.

Recommendation 12 – We recommend [redacted] management implement a system of quality control to ensure the timely completion of quarterly privileged user access reviews in accordance with USDA Departmental Regulation 3505-003.

Recommendation 13 – We recommend that Departmental Administration Information Technology Office management develop, document, and implement a control to monitor the assigned organization security coordinators complete privileged user access reviews in a timely manner.

Finding 8: Issues with timely producing an active user listing

DAITO management were not initially able to provide an active user listing for 1 of 10 USDA-operated systems selected for testing that includes relevant data elements, such as user's first name, last name, account creation date, and roles or privilege. While a complete system listing was eventually provided, this was not until system management was presented with a potential finding. Furthermore, we noted that similar issues with generating a user listing was experienced in FY 2023 by the team conducting the annual security control assessment a POA&M was created to track the system's inability to generate such a listing.

We determined the issue was caused by system representatives who we initially met with lacking the necessary training and expertise required to generate the user listing. More specifically, their proficiency in using the managerial reports and tools was insufficient, resulting in their inability to generate what should be considered a standard user listing. Furthermore, since DAITO management is not actively monitoring their POA&Ms, they were unaware that the previous incident involving the security control assessment team was being tracked as an ongoing deficiency.

The Government Accountability Office's Standards for Internal Control in the Federal Government requires entities, such as USDA, to develop and maintain readily available evidence of their implementation of their internal control systems. The inability to promptly generate a user listing for an application increases the risk that management will be unable to identify unauthorized users and inappropriate granting of system privileges (excessive privileges).

Recommendation 14 – We recommend Departmental Administration Information Technology Office management configure the system to generate user listings with the required data elements (e.g., first name, last name, account creation date, and roles or privileges) to support its system of internal controls and operational needs.

Recommendation 15 – We recommend Departmental Administration Information Technology Office management provide training to personnel supporting the application on system administration including their responsibilities in supporting access controls, audits, and assessments.

Recommendation 3 is also applicable to this finding regarding timely remediation of vulnerabilities.

Finding 9: Audit logs were not configured to retain historical audit data

We determined 1 of 10 USDA-operated systems selected for testing was not configured to retain historical audit data for privileged and non-privileged users. [redacted] [redacted] [redacted] management indicated they were aware of the deficiency, had already self-identified it as an POA&M, and were tracking remediation. The deficiency occurred because [redacted] management failed to prioritize resources to configure the system to retain historical audit data for both privileged and non-privileged users.

DR 3575-003, *Information Systems Log Retention*, July 7, 2022, requires that USDA Mission Areas, agencies, and staff offices configure systems and tools to collect logs needed to support investigations, event reconstruction, metrics, and research. Failure to configure a system to capture and collect both privileged and non-privileged security events may result in delayed identification, handling, review, and resolution of security events.

Recommendation 16 – We recommend [redacted] management enable the collection of privileged and non-privileged audit logging events and design and implement a process for monitoring and analyzing significant events for unauthorized or unusual activities.

Security Training

Security training encompasses both general awareness training for all users and specialized, role-based training for individuals with significant IT security responsibilities. It requires both regular IT users and privileged users to have the knowledge to perform their jobs appropriately, using information system resources without exposing the organization to unnecessary risk. It also requires USDA to create plans to address all identified skill gaps through its workforce assessment. We determined that USDA's security training maturity level was Consistently Implemented (Level 3). USDA can improve security in this domain by resolving the following issue:

Finding 10: Role Based Security Training not completed in a timely manner

USDA needs to implement its control requiring individuals with significant information security responsibilities to complete the required role-based security training (RBST) within 45 days of initial assignment and annually thereafter. Specifically, we determined:

- 1 of 15 new users did not complete their RBST training within 45 days of initial assignment. [redacted]
- 4 of 45 individuals did not complete their RBST training within 45 days after completing their last annual training. However, as of April 18, 2024, all 4 individuals have since completed the required training.

DR 3545-001, *Information Security Awareness Program*, October 25, 2023, requires USDA personnel with significant information security responsibilities to complete RBST training prior to accessing systems or annually thereafter.

CPOC management indicated that ongoing adjustments are being made because of the program's recent restructuring. Specifically, FY 2023 was the first year RBST was implemented at the Department-level, whereas previously it was managed and tracked separately by each mission area. Failure to ensure that all personnel with significant IT responsibilities complete the required training may result in these individuals not being able to perform their assigned duties or engage in inappropriate or unsafe activities. As a result, there is an increased risk the USDA's information systems and information could be exposed to cyber-attacks and threaten the integrity, availability, and confidentiality of sensitive data.

This occurred because Departmental policy does not specify repercussions for non-completion of the RBST within the 45-day timeframe. According to NIST SP 800-53 Rev. 5,[19] Federal agencies, like USDA, are required to enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies. As a result, following up with non-compliant individuals was deemed labor-intensive and prone to human error.

Recommendation 17 – We recommend Cybersecurity and Privacy Operations Center management update existing policies and procedures to include repercussions when an individual does not complete their required role-based security training in the designed 45-day time frame.

Recommendation 18 – We recommend Cybersecurity and Privacy Operations Center management develop a mechanism to track the completion of role-based security training and verify remedial action has occurred in the event an individual has not taken the training on a timely basis.

Information Security Continuous Monitoring

The purpose of the information security continuous monitoring domain is to ensure the ongoing monitoring and assessment of information systems and their control environments, with the goal of identifying and responding to security risks and vulnerabilities. ISCM helps organizations maintain an accurate understanding of their security posture, detect, and respond to security incidents in a timely manner, and make informed risk management decisions. Our performance audit determined that USDA's information security continuous monitoring maturity level was Managed and Measurable (Level 4). To improve security in this domain, USDA should address the following issue:

Finding 11: Outdated security program information was maintained, and annual security controls assessment was not completed

For 1 of 10 USDA-operated systems selected for testing, we identified the following weaknesses with its security program information:

- A security assessment plan has not been completed since FY 2022.
- A security controls assessment has not been completed since FY 2021.
- The last System Security Plan (SSP) was reviewed and updated on October 18, 2022.

USDA Seven Step Risk Management Framework (RMF) Process Guide, Revision 4.0, dated September 2019, requires security assessment plans to be reviewed and approved prior to a security controls assessment. Security controls assessments are performed on an annual basis. In addition, USDA ISCM Implementation Plan SOP, dated November 27, 2023, requires SSPs to be continually updated as a living document, but at least annually.

DAITO management attributed these findings to a lack of resource availability and budget constraints.

[19] NIST SP 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, December 10, 2020.

Without complete and up-to-date security control assessments, critical risks may not be identified, monitored, or mitigated. This could increase the risk to the confidentiality, integrity, and availability of the information system and the data within. Furthermore, there is a risk the Authorizing Official (AO) for the system may inadvertently re-authorize the system based on outdated security program information and without a complete understanding of whether sufficient controls are in place to mitigate existing risks to the system.

Recommendation 19 – We recommend Departmental Administration Information Technology Office management enforce the requirements for information system security documentation to be updated, reviewed, and approved in accordance with USDA policy. When annual security requirements cannot be completed within the required timeframe, ensure a formal risk waiver is procured.

Recommendation 20 – We recommend Departmental Administration Information Technology Office management conduct annual security control assessments in accordance with USDA's continuous monitoring schedule.

Recommendation 21 – We recommend Departmental Administration Information Technology Office management increase the resources dedicated to the assessment and authorization program, as needed, to completely execute all aspects of the program requirements on an on-going basis.

Recommendation 22 – We recommend Departmental Administration Information Technology Office management implement changes in operations, management, and oversight that enforces USDA requirements for the timely completion of security assessment plans.

Contingency Planning

Federal entities, including USDA, are required to prepare for events that may impact their mission and the availability of their information systems. This involves identifying and preparing against possible risks by developing a contingency plan to address a loss of system availability. Furthermore, the system owner is responsible for conducting annual testing of the contingency plan for the information system. We determined that USDA's contingency planning maturity level was Consistently Implemented (Level 3). USDA can improve security in this domain by resolving the following issue:

Finding 12: Weaknesses identified with contingency planning documentation

During our system-level testing, we identified weaknesses with the contingency plans and business impact analysis (BIAs) that were not developed, reviewed, or updated in a timely manner. Out of the 10 USDA -operated systems selected for testing , the ISCP's for 3 systems have not been updated and approved since FY 2022. Furthermore, the BIA for 1 of the 10 systems had also not been updated and approved since FY 2022. It should be noted that management had already self-identified and were tracking this deficiency for 2 of the 3 out-of-date ISCPs.

According to DR,[20] ISCPs and BIAs are required to be reviewed and updated at least annually. Failure to consistently update ISCPs increases the risk that USDA will be inadequately prepared to recover its systems after unplanned shutdowns and minimize business disruptions.

The contingency planning weaknesses were attributed to a variety of reasons. For one system, management failed to prioritize resources to address known vulnerabilities, including updating ISCPs. For another system, there was a lack of management oversight which resulted in the ISCP not being signed and mistakenly uploaded to the official USDA document repository. This oversight went unnoticed until the system was selected for an audit, at which point the system's management became aware of and addressed the discrepancy. Lastly, for the third system, management purposefully delayed completion of the ISCP/BIA until the system's FIPS 199 categorization is finalized. The system is being evaluated for a higher FIPS 199 categorization and a decision is expected to be made before the calendar year 2024 assessment begins.

Recommendation 23 – We recommend Office of the Chief Information Officer management establish a system of quality control to review all artifacts uploaded to the USDA document repository, ensuring their completeness, timeliness, and adherence to USDA requirements.

Recommendation 24 – We recommend [redacted] management complete a review and update of the [redacted] Information System Contingency Plan within the timeframe prescribed by DR 3571-001.

Recommendation 25 – We recommend [redacted] management finalize the system's security categorization and update the information system contingency plan and business impact analysis documents to align with the system's new categorization requirements.

[20] DR 3571-001, Information System Contingency Planning and Disaster Recovery Planning, dated June 1, 2016.

Conclusion

We determined that the overarching cause for several deficiencies was a lack of resources, including the use of significantly outdated technologies, insufficient staffing, and planning and coordination. These resource constraints were observed to be pervasive across the selected mission areas and program offices and impacted both USDA-operated and contractor-operated systems. [redacted] These factors have hindered USDA's ability to effectively modernize its systems and meet the evolving demands of its wide user base. To address the overarching cause, we are making one last recommendation to the CIO.

Recommendation 26 – We recommend the Chief Information Officer perform a cybersecurity resource assessment to identify any technology, people, or tool gaps.

Consistent with the FISMA requirements, OMB policy and guidance, and NIST standards and guidance, USDA established and maintained its information security program and practices for the five Cybersecurity Functions and nine FISMA Metric Domains. We reported 12 deficiencies noted within 4 of the 5 FISMA Cybersecurity Functions (Identify, Protect, Detect, and Recover) and in 7 of the 9 FISMA Metric Domains (RM, SCRM, CM, IAM, ST, ISCM, and CP). We made 26 recommendations related to these findings that, when implemented, should strengthen USDA's information security program if effectively addressed by management. To improve the maturity of its information security program, USDA should consider applying these recommendations to its entire universe of systems.

Of 29 previously open recommendations identified during the FY 2021, FY 2022, and FY 2023 performance audits, we determined that 1 recommendation remained open, 1 recommendation was partially implemented and that 27 recommendations were successfully closed by USDA and the issues did not recur during the performance audit period. One outstanding recommendation related to the IAM FISMA Metric Domain, and the other outstanding recommendation related to both RM, and DPP Metric Domains.

As a result, we assessed USDA's information security program as Consistently Implemented (Level 3), which was ineffective according to OMB's FY 2024 IG FISMA Reporting Metrics guidance. USDA should implement robust monitoring capabilities to continually assess the

[redacted]

[redacted]

security state of its systems to include a process to hold service centers accountable for identified compliance gaps.

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

Appendix I: Glossary of Terms

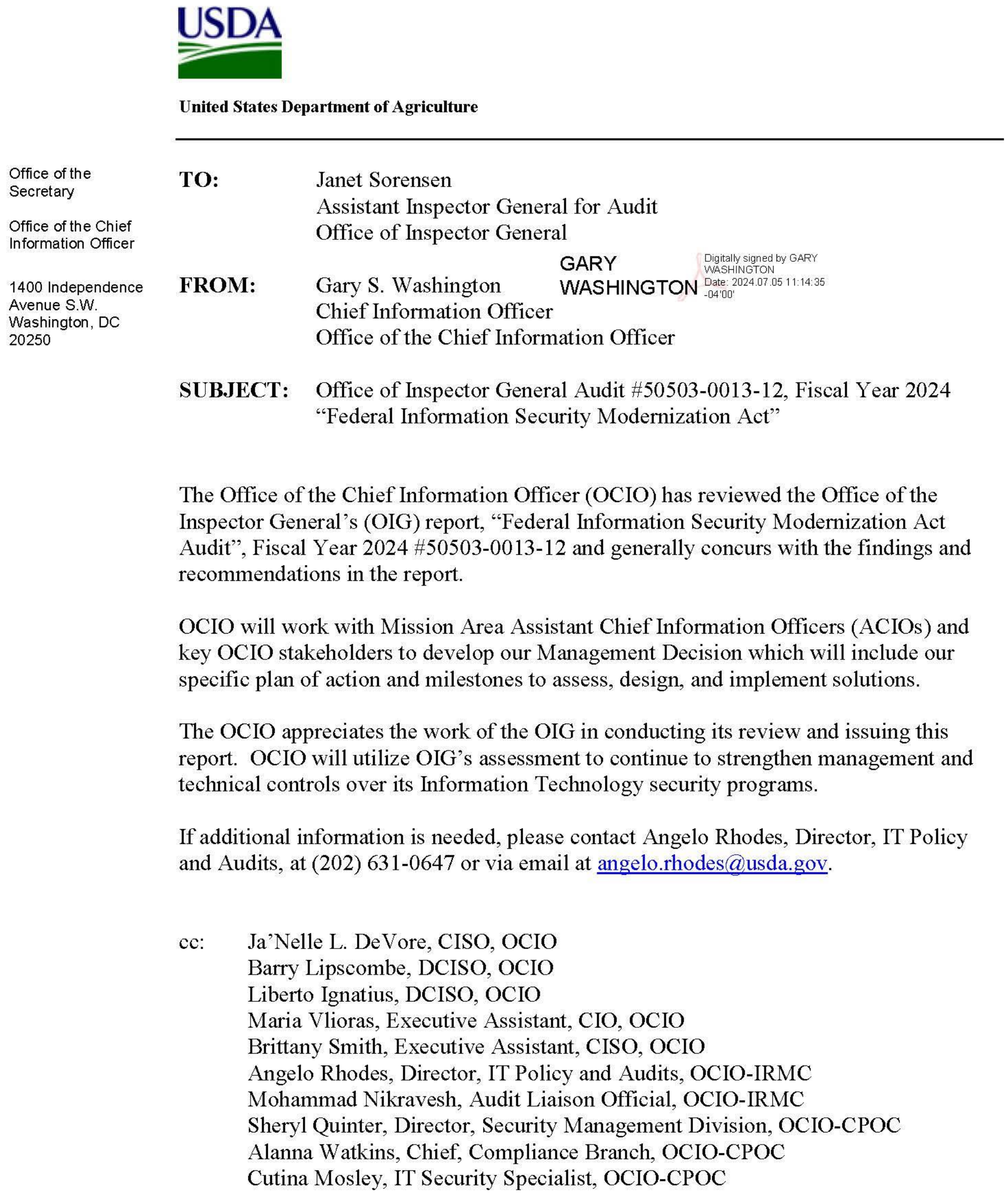
AICPA	American Institute of Certified Public Accountants
AO	Authorizing Official
ATO	Authorization to Operate
A&A	Assessment and Authorization
BIA	Business Impact Analysis
CEC	Client Experience Center
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CISA	Cybersecurity and Infrastructure Security Agency
CM	Configuration Management
CP	Contingency Planning
CPOC	Cybersecurity & Privacy Operations Center
CSAM	Cyber Security Assessment and Management
Cybersecurity Framework	National Institute Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity
DAITO	Departmental Administration Information Technology Office
DHS	Department of Homeland Security
DISC	Digital Infrastructure Services Center
DPP	Data Protection and Privacy
DR	Departmental Regulation
FISMA	Federal Information Security Modernization Act of 2014
[redacted]	[redacted]
FY	fiscal year
FY 2024 IG FISMA Metrics	Fiscal Year 2024 Inspector General Information Security Modernization Act of 2014 Reporting Metrics
GAGAS	Generally Accepted Government Auditing Standards
HVA	High-Value Asset
IAM	Identity and Access Management
ICT	Information and Communication Technology
IR	Incident Response
ISA	Interconnection Security Agreement
ISCM	Information Security Continuous Monitoring
IT	Information Technology
KPMG	KPMG LLP
MFA	Multi-Factor Authentication
[redacted]	[redacted]
NIST	National Institute of Standards and Technology
[redacted]	[redacted]
OCIO	Office of the Chief Information Officer
OCFO	Office of the Chief Financial Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones

RBST	Role Based Security Training
Rev.	Revision
RM	Risk Management
RMF	Risk Management Framework
[redacted]	[redacted]
SCRM	Supply Chain Risk Management
SP	Special Publications
SSP	System Security Plan
ST	Security Training
U.S.	United States
USDA	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 2024 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics (pages 28-56); and
Appendix III—Status of Prior Recommendations (pages 57-61).

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
Chief Information Officer
Office of the Chief Information Officer

GARY WASHINGTON
Digitally signed by GARY WASHINGTON
Date: 2024.07.05 11:14:35 -04'00'

SUBJECT: Office of Inspector General Audit #50503-0013-12, Fiscal Year 2024 "Federal Information Security Modernization Act"

The Office of the Chief Information Officer (OCIO) has reviewed the Office of the Inspector General's (OIG) report, "Federal Information Security Modernization Act Audit", Fiscal Year 2024 #50503-0013-12 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.

If additional information is needed, please contact Angelo Rhodes, Director, IT Policy and Audits, at (202) 631-0647 or via email at angelo.rhodes@usda.gov.

cc: Ja'Nelle L. DeVore, CISO, OCIO
Barry Lipscombe, DCISO, OCIO
Liberto Ignatius, DCISO, OCIO
Maria Vlioras, Executive Assistant, CIO, OCIO
Brittany Smith, Executive Assistant, CISO, OCIO
Angelo Rhodes, Director, IT Policy and Audits, OCIO-IRMC
Mohammad Nikravesh, Audit Liaison Official, OCIO-IRMC
Sheryl Quinter, Director, Security Management Division, OCIO-CPOC
Alanna Watkins, Chief, Compliance Branch, OCIO-CPOC
Cutina Mosley, IT Security Specialist, OCIO-CPOC

Learn more about USDA OIG at https://usdaoig.oversight.gov
Find us on LinkedIn: US Department of Agriculture OIG
Find us on Twitter: @OIGUSDA

Report suspected wrongdoing in USDA programs:
https://usdaoig.oversight.gov/hotline

Toll-free: 800-424-9121

In Washington, DC: 202-690-1622

All photographs on the front and back covers are from Adobe Stock with a licensing agreement.
They do not depict any particular audit, inspection, or investigation.

U.S. Department of Agriculture (USDA) is an equal opportunity provider, employer, and lender.

In accordance with Federal civil rights law and USDA civil rights regulations and policies, the USDA, its Agencies, offices, and employees, and institutions participating in or administering USDA programs are prohibited from discriminating based on race, color, national origin, religion, sex, gender identity (including gender expression), sexual orientation, disability, age, marital status, family/parental status, income derived from a public assistance program, political beliefs, or reprisal or retaliation for prior civil rights activity, in any program or activity conducted or funded by USDA (not all bases apply to all programs). Remedies and complaint filing deadlines vary by program or incident.

Persons with disabilities who require alternative means of communication for program information (e.g., Braille, large print, audiotape, American Sign Language, etc.) should contact the responsible Agency or USDA's TARGET Center at (202) 720-2600 (voice and TTY) or contact USDA through the Federal Relay Service at (800) 877-8339. Additionally, program information may be made available in languages other than English.

To file a program discrimination complaint, complete the USDA Program Discrimination Complaint Form, AD-3027, found online at How to File a Program Discrimination Complaint and at any USDA office or write a letter addressed to USDA and provide in the letter all of the information requested in the form. To request a copy of the complaint form, call (866) 632-9992. Submit your completed form or letter to USDA by: (1) mail: U.S. Department of Agriculture, Office of the Assistant Secretary for Civil Rights, 1400 Independence Avenue, SW, Washington, D.C. 20250-9410; (2) fax: (202) 690-7442; or (3) email: program.intake@usda.gov.