U.S. Department of Agriculture
Office of Inspector General

Evaluation of Plan of Action and Milestones (POA&Ms) Process

January 2026

Inspection Report 50501-0028-12

IMPORTANT NOTICE

This report contains sensitive information that is being withheld from public release due to concerns about the risk of circumvention of law.

Evaluation of Plan of Action and Milestones (POA&Ms) Process

Inspection Report 50501-0028-12

We determined that USDA agencies and offices did not record required information or promptly address cybersecurity vulnerabilities, [redacted]

OBJECTIVE

Our objective was to evaluate aspects of the Plan of Action and Milestones (POA&Ms) process used to reduce identified vulnerabilities.

BACKGROUND

USDA relies extensively on information technology to accomplish its mission. However, improving information technology and cybersecurity remains a top management challenge. To meet Federal requirements, USDA established a process to identify, assess, prioritize, and monitor the progress of corrective actions for security vulnerabilities—known as POA&Ms.

REVIEWED

Our scope period covered October 2023 to May 2025 in which we reviewed POA&M data from USDA's system of record.

WHAT OIG FOUND

In our review of the U.S. Department of Agriculture's (USDA) Plan of Action and Milestones (POA&Ms) process. Specifically, we found that USDA agencies and offices were not recording the required information necessary to facilitate the timely remediation of cybersecurity vulnerabilities—such as project completion dates and task milestones—in USDA's security system of record. Furthermore, the Office of the Chief Information Officer (OCIO) did not ensure that agencies and offices promptly addressed cybersecurity vulnerabilities. This occurred because OCIO: (1) did not establish oversight controls to ensure that required documentation is consistently updated in the system of record; and (2) did not establish alternative measures that could be implemented until sufficient resources could be obtained. [redacted]

WHAT OIG RECOMMENDS

We recommend that OCIO establish: [redacted]

OCIO officials agreed with our finding and recommendations. OIG accepted management decision for the two recommendations.

USDA OFFICE OF INSPECTOR GENERAL
United States Department of Agriculture

DATE: January 14, 2026

INSPECTION NUMBER: 50501-0028-12

TO: Samuel Berry
Chief Information Officer
Office of the Chief Information Officer

ATTN: Sherry Golden
Audit Liaison Official
IT Policy and Audits Division(IPAD)

FROM: Yarisis Rivera-Rojas
Acting Assistant Inspector General for Audit

YARISIS RIVERA ROJAS

Digitally signed by YARISIS RIVERA ROJAS
Date: 2026.01.14 09:48:09 -05'00'

SUBJECT: Evaluation of Plan of Action and Milestones (POA&Ms) Process

This report presents the results of our inspection of Evaluation of Plan of Action and Milestones (POA&Ms) Process. Your written response to the official draft is included in its entirety at the end of the report. Based on your written response, we are accepting management decision for the two recommendations in the report, and no further response to this office is necessary.

In accordance with Departmental Regulation 1720-1, final action needs to be taken within 1 year of the date of each management decision. Please follow your internal agency procedures in forwarding final action correspondence to the Office of the Chief Financial Officer.

We appreciate the courtesies and cooperation extended to us by members of your staff during our fieldwork and subsequent discussions. This report contains publicly available information and only publicly available information will be posted to our website (https://usdaoig.oversight.gov) in the near future.

Table of Contents

Background and Objective

Background

The U.S. Department of Agriculture (USDA) relies extensively on information technology (IT) resources to accomplish its mission. USDA systems support bird flu response, forest fires, global trade, and other key functions that drive the more than $1.5 trillion food and agriculture economy. According to the 2025 Federal IT Dashboard,[1] USDA spent more than $2.7 billion on IT related initiatives. However, improving IT and cybersecurity remains a top management challenge and a significant investment considering the emerging challenges and threats, such as malicious cyber operations against food processors and attacks against the agricultural supply chain.

OMB directs Chief Information Officers (CIOs) and agency program officials to develop, implement, and manage a Plan of Action and Milestones (POA&Ms) for all programs and systems they operate and control as part of compliance with the Federal Information Security Modernization Act (FISMA).[2] A POA&M equally describes actions taken or planned by the information system owner to correct deficiencies in the security controls and addresses remaining vulnerabilities in the information system (system owners may choose to: transfer, share, mitigate, avoid, or accept the vulnerabilities).

FISMA requires Federal agencies to develop and implement a process to document and remediate cybersecurity weaknesses. The National Institute of Standards and Technology (NIST) publication[3] further states that agencies must develop POA&Ms for their information systems to document planned and remedial actions so that security weaknesses or deficiencies can be corrected and known vulnerabilities[4] on the network are reduced or eliminated. The publication also notes that organizations should employ automated mechanisms to ensure that POA&Ms are accurate, up to date, and readily available. The automated mechanism and system of record that USDA utilizes is the Cyber Security Assessment and Management (CSAM)[5] which includes step-by-step procedures[6] for employees to follow. These procedures are summarized below in Table 1.

[1] The U.S. General Services Administration's Federal IT Dashboard enables agencies, the Office of Management and Budget (OMB), Congress, the Government Accountability Office, and the public to understand the value of their Federal IT portfolios, manage the health of their IT investments, and make better IT planning decisions.

[2] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073–3088 (codified at 44 U.S.C. § 3551-3558).

[3] NIST Special Publication (SP) 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations* (NIST SP 800-53) (Sept. 2020).

[4] NIST SP 800-37, Rev. 2, *Risk Management Framework for Information Systems and Organizations* (Dec. 2018) defines *vulnerability* as a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

[5] USDA utilizes a POA&Ms tracking system called CSAM. This system is maintained by the U.S. Department of Justice and is designed to help Federal agencies streamline their compliance and security processes. CSAM streamlines and standardizes POA&M processes across the organization to leverage POA&M creation, status workflows, control associations, completion tracking, and notifications.

[6] USDA Information Security Division & Security Management Division, *Standard Operating Procedures (SOPs) on Plan of Action & Milestones (POA&M) Management*, version 1.3 (Sept. 2021).

Table 1: Summary of the POA&Ms Process

Phase	Activities
Create	• Identify weakness noted during assessment or audit • Assign individuals to be responsible • Determine criticality and risk level • Document milestones • Calculate estimated cost • Determine the scheduled completion dates • Approve POA&M for implementation
Remediate	• Determine whether to accept risk rather than remediate • Verify actions addressed identified weakness • Provide evidence to support completion • Validate all milestones are complete
Review	• Ensure POA&Ms are properly managed and remediated • Conduct monthly reviews of closed POA&Ms • Re-open POA&Ms with insufficient evidence

Table 1: Summarizes the procedures for USDA employees to follow for the POA&Ms process. Table by the Office of Inspector General (OIG).

To meet FISMA and NIST requirements, USDA developed a departmental regulation,[7] which establishes the policy for identifying, assessing, prioritizing, and monitoring the progress of corrective actions for cybersecurity vulnerabilities found in USDA programs, applications, and systems.

Roles and Responsibilities in the POA&Ms Process

System owners have a significant role in the mitigation of POA&Ms, primarily managing prompt resolution of identified weaknesses and control deficiencies as well as maintaining accurate records. The Office of the Chief Information Officer (OCIO) is responsible for the overall oversight of the POA&Ms by establishing policies and procedures, ensuring compliance, and reporting annually to the Secretary on the program's effectiveness. Agency and Staff Office CIOs assess and monitor all identified vulnerabilities within their agency, ensure adequate resources and funding are allocated, and ensure corrective actions are taken to resolve all identified vulnerabilities related to their respective mission areas. All mission area decisions to accept information security risk are subject to oversight by OCIO.

[7] USDA Departmental Regulation 3565-003, *Plan of Action and Milestones Policy* (Sept. 25, 2013).

In response to identified vulnerabilities, Federal agencies can take the following actions:

- Acceptance
- Transfer
- Share
- Mitigation (could include compensating controls)
- Avoidance

Compensating Controls to Mitigate Vulnerabilities

Compensating controls can serve as a valuable tool to ensure timely mitigation. USDA may support customers that utilize legacy systems[8] that have inherent vulnerabilities. Management may make the decision to retain the system on the network for business reasons. When such a decision is reached, according to USDA and Federal policy, the rationale should be documented, and the risk should be accepted. USDA utilizes a risk-based decision form to facilitate the risk acceptance process; the form is comprehensive and includes whether the decision was made with or without compensating controls. [9]

Objective

Our objective was to evaluate aspects of the Plan of Action and Milestones (POA&Ms) process used to reduce identified vulnerabilities.

[8] A legacy system refers to an outdated computer system, software, or technology still in use within an organization despite the availability of newer alternatives.

[9] USDA Information Security Center & Security Management Division, *Standard Operating Procedures (SOP) on Risk-Based Decision Management*, version 1.6 (Sept. 2021).

Finding 1: USDA Needs to Improve Its POA&Ms Remediation Process

OCIO did not ensure that USDA agencies and offices promptly addressed cybersecurity vulnerabilities identified during reviews. Furthermore, USDA agencies and offices were not recording the required information necessary to facilitate the timely remediation of cybersecurity vulnerabilities—such as project completion dates and task milestones—in USDA's security system of record. This occurred because OCIO did not establish oversight controls to ensure that the required documentation is consistently updated in its system of record. Additionally, OCIO stated that a lack of agency resources impacted agencies and offices from timely remediating cybersecurity vulnerability; however, OCIO had not established alternative measures that could be implemented until sufficient resources could be obtained. [redacted]

NIST standards and USDA policy require the timely remediation of identified vulnerabilities, which are tracked through POA&Ms. The following information must be included in the POA&M: resources needed to address the identified vulnerabilities (including cost information), scheduled completion date, task milestones, as well as severity[10] and criticality.[11]

During our review of the POA&Ms process, we found that USDA had challenges with timeliness and accuracy of information recorded as noted below.

[redacted]

[redacted]

[redacted]

[10] *Severity* is the level of risk or potential damage associated with a security vulnerability, determined by its exploitability, impact of confidentiality, integrity, availability, and the context of the affected system. Severity is typically categorized (Low, Moderate, High, or Critical) based on standardized scoring systems like the Common Vulnerability Scoring System.

[11] *Criticality* is user identified based on the calculation of the likelihood of the event occurring and the impact of the failure.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Overall, OCIO officials acknowledged the need to improve the POA&Ms remediation process and data accuracy issues. OCIO generally concurred with our finding and recommendations.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Scope and Methodology

The scope of our inspection covered aspects of USDA's POA&Ms process used to reduce identified vulnerabilities from October 2023 to May 2025. We performed our inspection fieldwork from February 2025 to November 20, 2025. We did not perform on-site visits. We discussed the results of our inspection with agency officials on December 3, 2025, and included their comments, as appropriate.

To accomplish our inspection objective, we:

- Reviewed applicable regulations, guidance, policies, and procedures;
- Reviewed the universe of POA&Ms data in USDA's system of record from October 2023 to May 2025;
- Reviewed additional documentation relevant to the POA&Ms process; and
- Interviewed officials responsible for managing the POA&Ms process.

The inspection was conducted in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*.

Abbreviations

ACISO	Assistant Chief Information Security Officer
CIO	Chief Information Officer
CSAM	Cybersecurity Assessment and Management
FISMA	Federal Information Security Modernization Act
IT	information technology
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
POA&M	Plan of Action and Milestones
SOP	Standard Operating Procedure
SP	Special Publication
USDA	U.S. Department of Agriculture

OCIO's
Response to Inspection Report

United States Department of Agriculture

OFFICE OF THE CHIEF INFORMATION OFFICER

DATE: December 10, 2025

TO: Yarisis Rivera-Rojas
Assistant Inspector General for Audit
USDA Office of Inspector General

FROM: David Peters /s/
Deputy Chief Information Officer
Office of the Chief Information Officer

SUBJECT: Response to Recommendations in OIG Engagement No. 50501-0028-12

The Office of the Chief Information Officer (OCIO) submits the following response to the recommendations in the Office of Inspector General's (OIG) engagement 50501-0028-12, *Evaluation of Plan of Action and Milestones (POA&Ms) Process*.

[redacted]

[redacted]

If additional information is needed, please contact Renae Harris-Hill, Director, IT Policy and Audits, at (202) 993-6071 or via email at maryrenae.harris-hill@usda.gov.

cc: Samuel Berry, CIO, OCIO
Anthony Brannum, CISO, OCIO
Barry Lipscombe, DCISO, OCIO
Maria Tinker, Executive Assistant, CIO, OCIO
Brittany Smith, Executive Assistant, CISO, OCIO
Renae Harris-Hill, Director, IT Policy and Audits, OCIO-IRMC
Sherry Golden, Agency 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 X: @OIGUSDA

Report suspected wrongdoing in USDA programs:

https://usdaoig.oversight.gov/resources/hotline-information

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, USDA, its Agencies, offices, and employees, and institutions participating in or administering USDA programs and operations are prohibited from discriminating based on on race, color, national origin, age, disability, sex, religion, retaliation for engaging in protected civil rights activity or opposition to any practice made unlawful under any Federal antidiscrimination laws, or receipt of income derived from programs or activities conducted or funded by OIG, political beliefs, or marital, familial or parental status (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 aProgram 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 IndependenceAvenue, SW, Washington, D.C. 20250 9410; (2) fax: (202) 690-7442; or (3) email: program.intake@usda.gov.

Cover photos are from USDA Flickr and are in the public domain. They do not depict any particular audit, inspection, or investigation.