U.S. Department of Agriculture
Office of Inspector General

Cybersecurity of Artificial Intelligence Technology at USDA

May 2026

Inspection Report 50801-0018-12








Cybersecurity of Artificial Intelligence Technology at USDA

Inspection Report 50801-0018-12

We determined that USDA has not fully implemented cybersecurity and governance controls within Artificial Intelligence systems in compliance with federal standards, leaving the agency at risk of data breaches or reputational harm.

OBJECTIVE

Our objective was to determine if USDA has implemented cybersecurity controls within critical Artificial Intelligence (AI) systems in compliance with federal standards.

BACKGROUND

OMB is encouraging agencies to implement AI. AI refers to computer systems capable of performing complex tasks, such as reasoning, making decisions, or solving problems. The United States is at the forefront of AI development, and agencies must adopt a forward-leaning and pro-innovation approach that takes advantage of this technology to help shape the future of Government operations.

REVIEWED

We reviewed the Department's AI use case inventory for fiscal year 2024 to determine whether there were sufficient cybersecurity and governance controls commensurate with Departmental, federal, and statutory requirements.

WHAT OIG FOUND

The U.S. Department of Agriculture (USDA) has not fully implemented cybersecurity and governance controls within Artificial Intelligence (AI) systems (approved AI use cases). The Office of the Chief Information Officer (OCIO) has not adequately performed authorizations to operate (ATO) or risk assessments for all USDA AI use cases. Additionally, USDA is not in full compliance with federal standards related to AI. This occurred due to USDA's implementation process, which prioritized AI implementation over cybersecurity and governance controls outlined in federal guidance. As a result, USDA AI technologies could be vulnerable and lack critical security controls, leaving the agency susceptible to data breaches or reputational harm.

WHAT OIG RECOMMENDS

We recommend that OCIO: (1) implement controls and Department-wide regulations to ensure high-impact assessments of AI use cases are conducted in compliance with the Office of Management and Budget (OMB) requirements; (2) review and update all applicable policies and procedures to incorporate AI in compliance with OMB requirements; (3) develop and implement a process to continually review and update USDA's AI inventory; and (4) develop and implement a process to ensure a risk assessment, ATO determination, and an overall system impact analysis is conducted prior to AI technologies being permitted on the USDA network.

OCIO agreed with our finding and recommendations. We accepted management decision for all four recommendations.

DATE: May 12, 2026

INSPECTION NUMBER: 50801-0018-12

TO: Kimberly R. Jackson
Deputy Chief Information Officer
Office of the Chief Information Officer

ATTN: Sherry Golden
Audit Liaison Official
Office of the Chief Information Officer

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

YARISIS RIVERA ROJAS
Digitally signed by YARISIS RIVERA ROJAS
Date: 2026.05.12 14:37:47 -04'00'

SUBJECT: Cybersecurity of Artificial Intelligence Technology at USDA

This report presents the results of our inspection of Cybersecurity of Artificial Intelligence Technology at USDA. 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 all four 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 will be posted in its entirety to our website (https://usdaoig.oversight.gov) in the near future.

Table of Contents

Background and Objective

Background

The United States is at the forefront of Artificial Intelligence (AI) development, and agencies must adopt a forward-leaning and pro-innovation approach that takes advantage of this technology to help shape the future of Government operations. To sustain and enhance America's global dominance in AI and promote human flourishing, economic competitiveness, and national security, the President issued Executive Order 14179.[1] To implement the Executive Order the Office of Management and Budget (OMB) issued Memorandum M-25-21. See the *Key Definitions* for terms related to AI.

KEY DEFINITIONS:

AI
AI refers to computer systems capable of performing complex tasks, such as reasoning, making decisions, or solving problems. It describes a wide range of technologies, including generative AI, which is capable of producing original content in response to user input. The benefits of AI include increased efficiency, decreased operational costs, and quick generation of content.

Shadow AI
Shadow AI is the unsanctioned use of any Departmental AI tool or application by employees or end users without the formal approval or oversight of the information technology (IT) department.

AI Use Case
AI use cases are specific scenarios in which AI is designed, developed, procured, or used to advance the execution of agencies' missions and their delivery of programs and services, enhance decision making, or provide the public with a particular benefit.

OMB's guidance encourages agencies to harness solutions that bring the best value to taxpayers, increase quality of public services, and enhance Government efficiency. Under this guidance, the U.S. Department of Agriculture (USDA) is directed to develop effective policies and processes for the timely deployment of AI to accelerate the federal use of AI by focusing on three key priorities: innovation, governance, and public trust.[2]

While there are benefits to implementing AI, AI technologies pose risks that can negatively impact individuals, groups, and organizations. Like other types of technology, AI risks can emerge in a variety of ways and can be characterized as long- or short-term, high- or low-probability, systemic or localized, and high- or low-impact. These risks make AI a uniquely challenging technology for organizations and society to deploy and use. Without proper controls, AI systems can amplify, perpetuate, or exacerbate undesirable outcomes for individuals and organizations.

If the applicable laws and guidance are not followed, there is an increased risk of Shadow AI.[3] Shadow AI is primarily derived from poor inventory controls; it can result in:

- unauthorized access to sensitive information,
- data breaches,

[1] Executive Order 14179, *Removing Barriers to American Leadership in Artificial Intelligence* (Jan. 23, 2025).
[2] OMB, *Accelerating Federal Use of AI through Innovation, Governance, and Public Trust*, Memorandum M-25-21 (Apr. 3, 2025).
[3] Shadow AI is the unsanctioned use of any AI tool or application by employees or end users without the formal approval or oversight of the IT department.

- accidental exposure of sensitive data, or data leaks, and
- significant reputational harm.

Effective oversight and controls are critical to protecting data and maintaining public trust. Examples of continuous AI improvement that can help mitigate these risks are illustrated below.

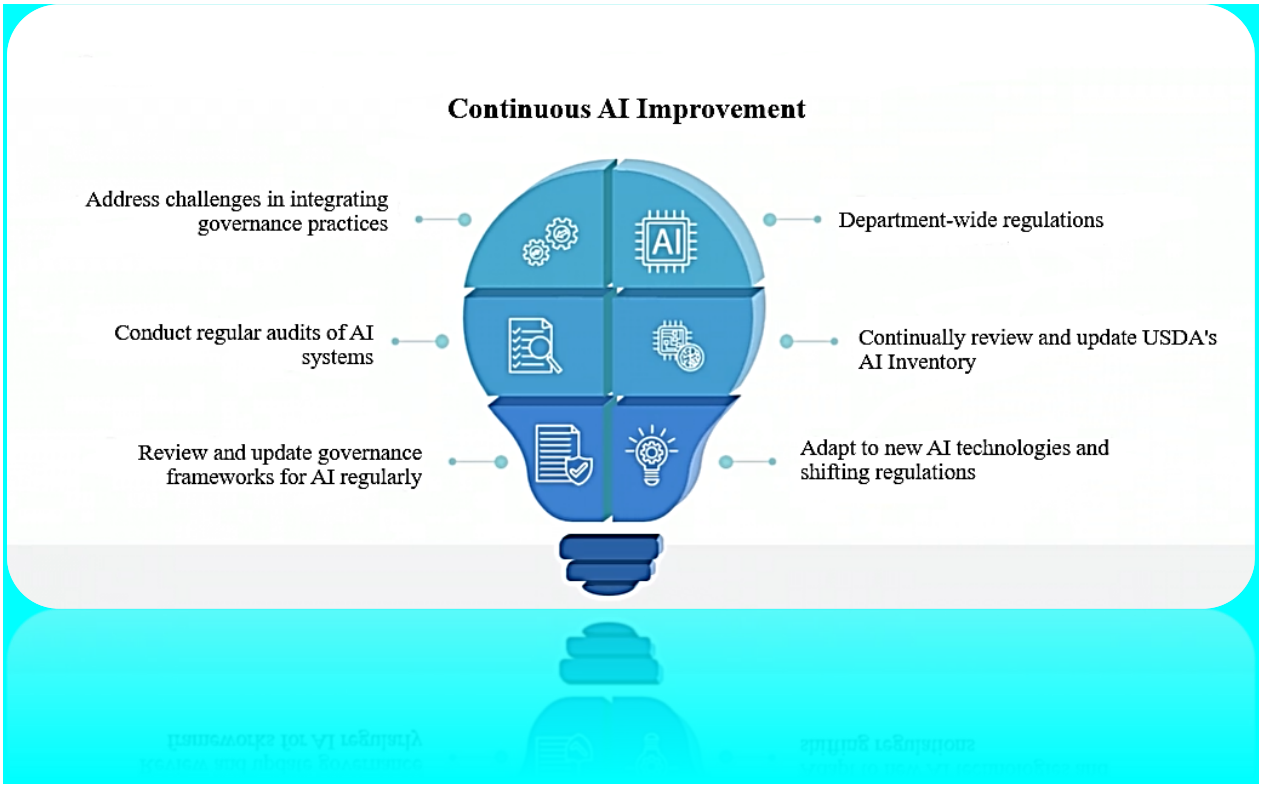


Figure 1: AI implementation best practices based on federal regulations and National Institute of Science and Technology (NIST) guidance. Graphic by the Office of Inspector General (OIG).

Objective

Our objective was to determine if USDA has implemented cybersecurity controls within critical Artificial Intelligence (AI) systems in compliance with federal standards.

Finding 1: USDA Should Improve Governance and Cybersecurity of AI Technologies

USDA has not fully implemented cybersecurity and governance controls within AI systems (approved AI use cases). The Office of the Chief Information Officer (OCIO) has not adequately performed authorizations to operate (ATO) or risk assessments for all USDA AI use cases. Additionally, USDA is not in full compliance with federal standards related to AI. This occurred due to USDA's implementation process, which prioritized AI implementation over cybersecurity and governance controls outlined in federal guidance. As a result, USDA AI technologies could be vulnerable and lack critical security controls, leaving the agency susceptible to data breaches or reputational harm.

OMB requires agencies to develop an AI strategy and compliance plan, update IT policies, maintain an AI use case inventory and implement minimum risk management practices for high-impact AI use cases.[4] Departmental Regulations (DRs) require all USDA IT systems to have an ATO prior to being placed into operation and that assessment and authorization (A&A) documentation be maintained in the Cyber Security Assessment and Management tool (CSAM).[5] These requirements, along with additional applicable federal laws, regulations, and guidance OIG used to assess USDA's compliance with AI standards, are summarized in Exhibit A.

Governance of AI Technology Should be Improved

While USDA achieved certain governance milestones it has not met several requirements outlined in OMB M-25-21. The following table summarizes USDA's compliance with selected AI directive requirements that were in scope during our review.

Status of AI Requirements Reviewed

Directive	Requirement	Implementation Deadline	Compliant (Yes/No)
OMB M-25-21	Appoint a Chief AI Officer within 60 days	June 2, 2025	**Yes**
OMB M-25-21	Develop Compliance Plans within 180 days	September 30, 2025	**Yes**
OMB M-25-21	Develop and publicly release an AI Strategy within 180 days	September 30, 2025	**Yes**
OMB M-25-21	Update Agency Policies within 270 days	December 29, 2025	**No**
OMB M-25-21	Develop a Generative AI Policy within 270 days	December 29, 2025	**No**

[4] OMB, *Accelerating Federal Use of AI through Innovation, Governance, and Public Trust*, Memorandum M-25-21 (Apr. 3, 2025).
[5] USDA DR 3540-003, *Security Assessment and Authorization* (Aug. 12, 2014).

Directive	Requirement	Implementation Deadline	Compliant (Yes/No)
OMB M-25-21	Publish an AI Use Case Inventory annually	Annually	**Yes**
OMB M-25-21	Implement minimum risk management practices for high-impact AI within 365 days	April 3, 2026	**No**

Table 1: USDA compliance with requirements of AI directives. Table by OIG.

A key element to AI governance under the OMB requirements is ensuring that agencies can identify and manage AI use cases that carry the highest risk. OIG selected a non-statistical sample of eight AI use cases and requested supporting documentation to determine whether a use case was high-impact.[6] Our sample selection was based on criteria for high-impact AI outlined in OMB M-25-21. OIG used the criteria and judgmentally selected use cases, based on the descriptions, where the output serves as a principal basis for decisions or actions that have a significant effect on:

- an individual or entity's civil rights or privacy;
- an individual or entity's access to critical Government resources or services;
- human health and safety; or
- critical infrastructure or public safety.

We found that OCIO had not performed or documented its reviews as required.

Furthermore, OMB M-25-21 requires agencies to update policies. The guidance requires agencies to revisit and update, where necessary, their internal policies on IT infrastructure, data, cybersecurity, and privacy to address AI. We requested AI policies and procedures and OCIO officials stated they have not updated or developed any policies or procedures.

Because the Department did not establish strong AI governance, the agency is at an increased risk of inappropriate use of AI tools, legal penalties, reputational harm, and data integrity issues.

USDA Does Not Have a Defined Process to Track AI Inventory

USDA identified 82 operational AI use cases for its 2024 inventory. However, we determined that the inventory could not be verified as complete and accurate due to the sole reliance on annual self-reporting being utilized to obtain USDA's AI inventory.

[6] OMB defines high-impact AI as AI with an output that serves as a principal basis for decisions or actions with legal, material, binding, or significant effect on (a) an individual or entity's access to education, housing, credit, employment, and other programs, (b) an individual or entity's access to critical Government resources or services, or (c) critical infrastructure or public safety.

Public Law 117–263 requires that agencies prepare and maintain an inventory of the agency AI use cases.[7] DR 3520-002 requires that USDA develop, document, and maintain a current, complete, and accurate inventory of each information system or service and its components under configuration control.[8]

To obtain its AI inventory, USDA conducts an annual data call (last conducted on September 2, 2025) that relies on AI use case owners to self-report applicable information for each use case. When the primary governance method is self-reporting, it can create a false sense of security that can lead to inaccurate inventory of AI tools, which can contribute to instances of Shadow AI. As AI implementation is becoming widespread, the inventory should be updated continuously to account for changes. Furthermore, not mitigating the risk of Shadow AI could lead to systems on the network that USDA is not aware of, which could result in data leakage.

USDA Should Improve the Cybersecurity of Its AI Technologies

We found that USDA AI use cases did not have an ATO, and A&A documentation was not maintained in the USDA CSAM tool. The ATO is the official management decision given by a senior agency official or officials to authorize operation of an information system.[9] The Federal Information Security Modernization Act (FISMA) requires federal agencies to develop and implement policies, plans, and procedures to continually assess the risk and magnitude of harm that could result from the unauthorized access or destruction of information or information systems.[10]

Departmental regulations state that all USDA IT programs, systems, and contractor-provided systems, including cloud systems and services, require an ATO. [11] AI systems without an ATO create vulnerabilities because management does not have assurance cybersecurity controls are in place. Authorizing officials are directed to review accreditation packages, specify any required changes, authorize systems for operation, and accept all operational risk. Authorized systems are required to be continually monitored for risk and A&A documentation maintained in CSAM. We found that:

- 73 of the 82 operational AI use cases did not have an ATO prior to operation and were not recorded in CSAM, and
- Of the nine AI use cases that have an ATO, two did not maintain required documentation in CSAM.

See Exhibit B for details of USDA's active AI use case inventory and their compliance with ATO requirements.

[7] Pub. L. No. 117-263, div. G, title LXXII, subtitle B, § 7225 (codified at 40 U.S.C. 11301 note) (Dec. 23, 2022).
[8] USDA DR 3520-002, *Configuration Management* (July 17, 2019).
[9] NIST Special Publication (SP) 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations* (Dec. 2018).
[10] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073–3088 (codified at 44 U.S.C. § 3551-3558).
[11] USDA DR 3540-003, *Security Assessment and Authorization* (Aug. 12, 2014).

USDA informed us they are exploring various methods to improve AI governance and cybersecurity, though none have final implementation dates as of March 2026. Examples include:

- a third-party AI product testing and validation contract to assist with compliance,
- process to identify systems that utilize AI and flag these systems in CSAM, and
- completion of an internal draft AI playbook documenting AI controls.

USDA will continue to implement AI technologies to support its mission and improve service to the American people. It is imperative that governance and cybersecurity controls over AI activities are top priorities. Governance provides the policies and oversight necessary to mitigate risks like bias and non-compliance, while cybersecurity controls protect AI models and data from unauthorized access or tampering. Going forward, USDA must ensure that governance and cybersecurity controls are factored in prior to deployment of AI use cases. Addressing cybersecurity and privacy issues after implementation is not only much more difficult and expensive, but it also exposes USDA to unnecessary risk.

Recommendation 1

Implement controls and Department-wide regulations to ensure high-impact assessments of AI use cases are conducted in compliance with OMB requirements.

Agency Response

OCIO agreed with the recommendation. OCIO will implement the AI Impact Assessment template developed by OMB and develop and implement a Department-wide regulation requiring this template for all AI use cases to determine level of impact.

OCIO provided an estimated completion date of September 30, 2026.

OIG Position

We accept management decision for this recommendation. For final action, OCIO needs to provide the Office of the Chief Financial Officer with a copy of the AI Impact Assessment template and the developed and published Department-wide regulation.

Recommendation 2

Review and update all applicable policies and procedures to incorporate AI in compliance with OMB requirements.

Agency Response

OCIO agreed with the recommendation. OCIO will review IT policies and procedures and determine whether updates are needed. Where updates are needed, revised policies

will be drafted and submitted for agency clearance. If necessary, interim guidance will be issued.

OCIO provided an estimated completion date of December 31, 2026.

OIG Position

We accept management decision for this recommendation. For final action, OCIO needs to provide the Office of the Chief Financial Officer with evidence of the review of IT policies and procedures and support for the determination decision for updates to policies and procedures.

Recommendation 3

Develop and implement a process to continually review and update USDA's AI inventory.

Agency Response

OCIO agreed with the recommendation. OCIO will implement an AI checklist for all IT procurements to identify where AI is being developed or adopted. The checklist will include confirmation that the use case has been entered into inventory and that an impact determination has been completed. The Chief AI Officer, or authorized delegate, will approve or deny submissions based on review of the checklist.

OCIO provided an estimated completion date of June 30, 2026.

OIG Position

We accept management decision for this recommendation. For final action, OCIO needs to provide the Office of the Chief Financial Officer with a copy of the developed and implemented AI checklist.

Recommendation 4

Develop and implement a process to ensure a risk assessment, ATO determination, and an overall system impact analysis is conducted prior to AI technologies being permitted on the USDA network.

Agency Response

OCIO agreed with the recommendation. OCIO will develop a process to review ATO'd systems, or new systems requiring an ATO, for the introduction of AI. Where AI is introduced, the Chief AI Officer and the Chief Information Security Officer will adopt a process with steps and timelines for reviewing the ATO and conducting an impact analysis. Where needed, a risk assessment will be conducted.

OCIO provided an estimated completion date of December 31, 2026.

OIG Position

We accept management decision for this recommendation. For final action, OCIO needs to provide the Office of the Chief Financial Officer with a copy of the process to review the ATO process for new and existing systems with AI introduced and the associated impact analysis.

Scope and Methodology

The scope of our inspection was Department-wide and focused on all 82 operational USDA AI use cases and the policies and guidance related to AI for fiscal year 2025. We performed our fieldwork remotely from July 2025 through March 2026. We non-statistically selected eight AI use cases for review to determine whether an analysis was performed to properly classify use cases as high-impact. Our sample selection was based on criteria for high-impact AI outlined in OMB M-25-21. OIG used the criteria and judgmentally selected use cases, based on the descriptions, where the output serves as a principal basis for decisions or actions that have a significant effect on:

- an individual or entity's civil rights or privacy;
- an individual or entity's access to critical Government resources or services;
- human health and safety; or
- critical infrastructure or public safety.

We discussed the results of our inspection with OCIO officials on April 23, 2026, and included their comments, as appropriate.

To meet our objective, we:

- Interviewed OCIO officials;
- Examined USDA's 2024 AI use case inventory for completeness and accuracy;[12]
- Reviewed federal laws and regulations and agency policy and procedures related to AI to determine USDA's compliance with statutory requirements;
- Reviewed executive orders, OMB guidance, and NIST standards to identify AI related requirements applicable to USDA; and
- Reviewed security controls for AI technologies to determine whether they complied with DRs to protect the confidentiality, integrity, and availability of USDA systems and data.

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

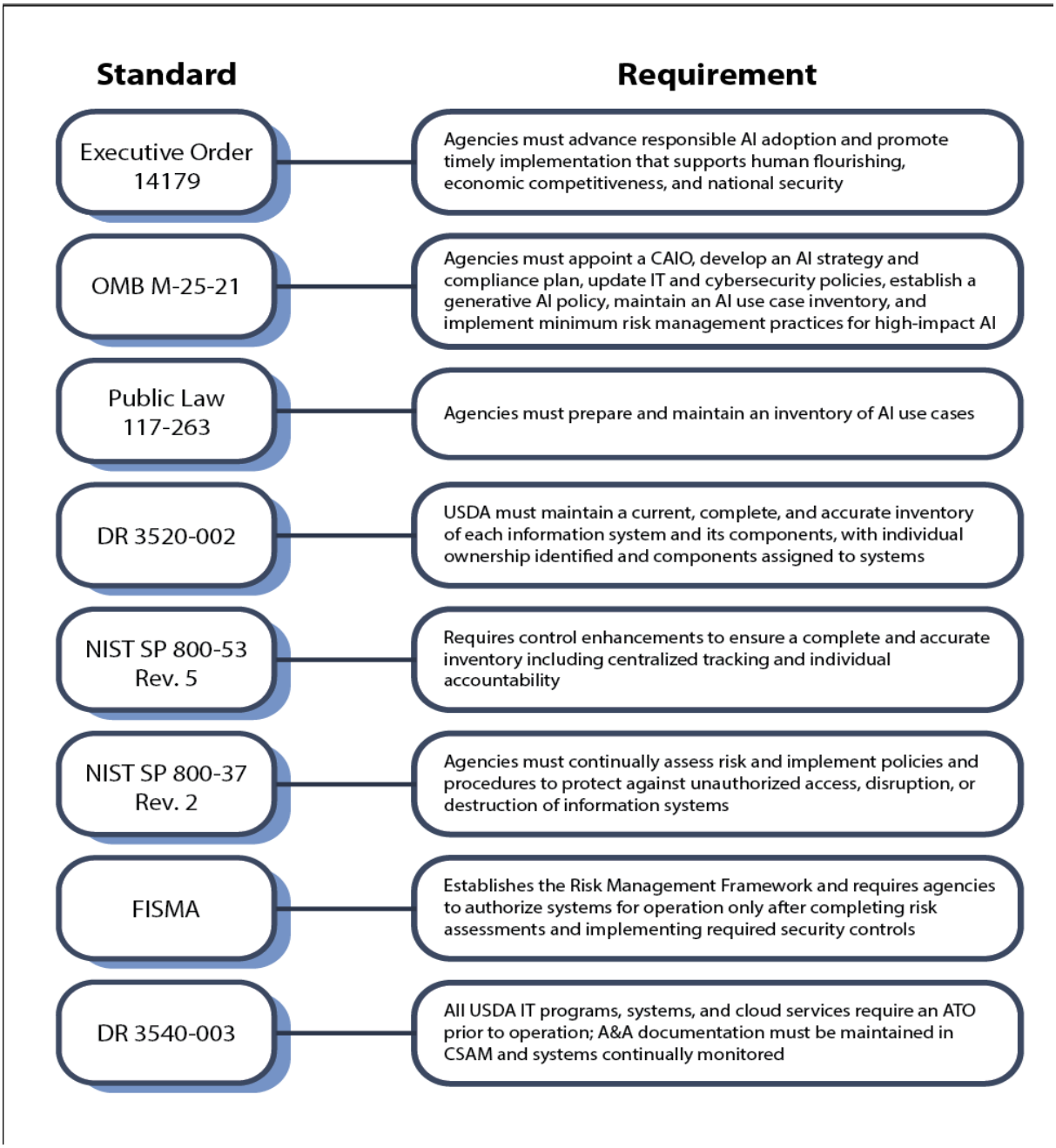
[12] The 2024 AI use case inventory was used because the 2025 AI use case inventory was not published until January 2026.

Abbreviations

A&A	Assessment and Authorization
AI	Artificial Intelligence
ATO	Authorization to Operate
CSAM	Cyber Security Assessment and Management
DR	Departmental Regulation
FISMA	Federal Information Security Modernization Act
IT	information technology
NIST	National Institute of Science and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
SP	Special Publication
USDA	U.S. Department of Agriculture

Exhibit A: Relevant Criteria Used to Assess the Department's Compliance with Requirements for AI

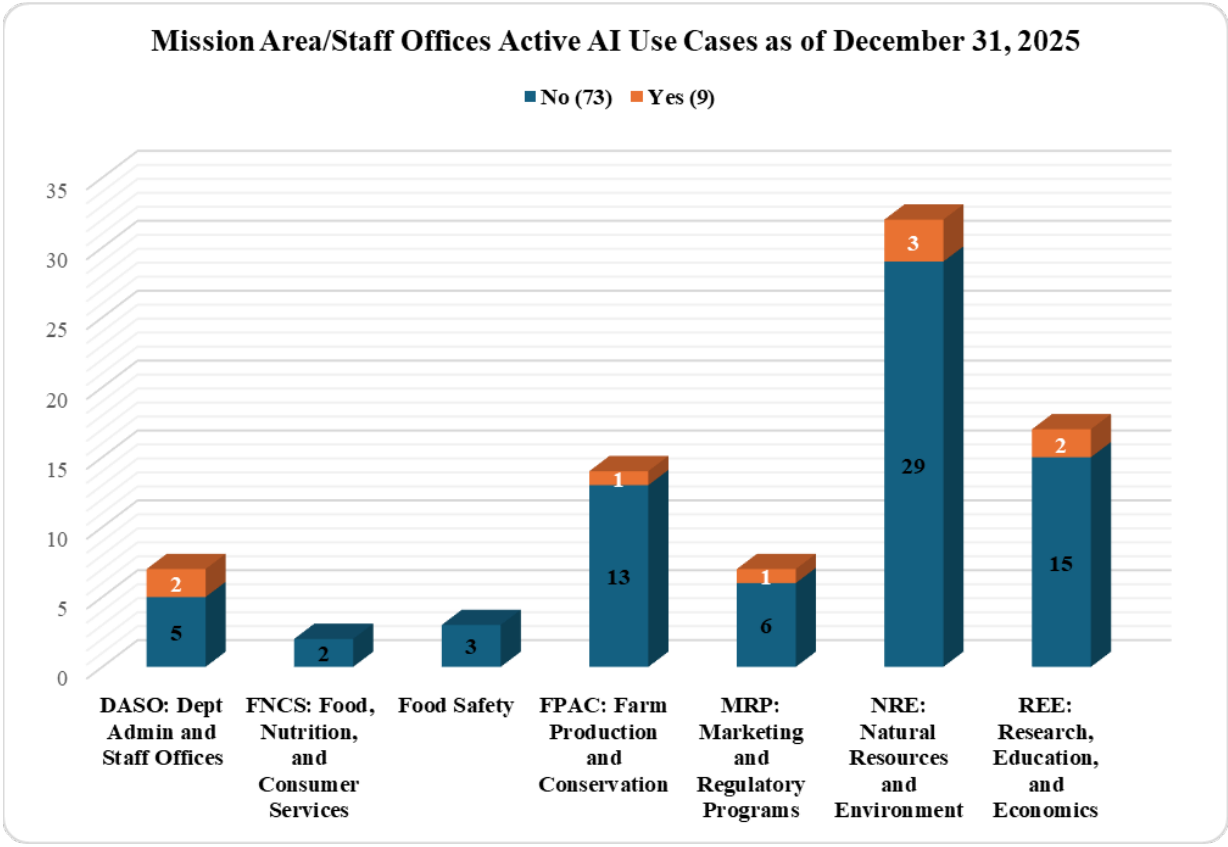
Exhibit A provides a visual presentation of applicable AI criteria and the related requirements for AI.



Graphic by OIG.

Exhibit B: System ATO Status for Active AI Use Cases

Exhibit B provides a visual presentation of active AI use case inventory and their compliance with having a required system ATO.



Graphic by OIG.

Office of the Chief Information Officer's Response to Inspection Report

United States Department of Agriculture

DATE: May 7, 2026

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

FROM: Kimberly R. Jackson /s/
Deputy Chief Information Officer
Office of the Chief Information Officer

SUBJECT: Response to Recommendations in OIG Engagement No. 50801-0018-12

The Office of the Chief Information Officer submits the following response to the recommendations in the Office of Inspector General's (OIG) engagement *Cybersecurity of Artificial Intelligence Technology at USDA*.

Recommendation 1: Implement controls and Department-wide regulations to ensure high-impact assessments of AI use cases are conducted in compliance with the Office of Management and Budget (OMB) requirements.

Agency Response:
Agree with recommendation: **X** Yes __ No
Agree with monetary results: __ Yes __ No **X** N/A

In response to this recommendation, the agency will implement the AI Impact Assessment template developed by OMB's Chief Artificial Intelligence Officer Council (CAIOC) and develop and implement a department-wide regulation requiring this template for all AI use cases to determine level of impact.

Completion or Estimated Completion Date: *Sept 30, 2026*

Recommendation 2: Review and update all applicable policies and procedures to incorporate AI in compliance with OMB requirements.

Agency Response:
Agree with recommendation: **X** Yes __ No
Agree with monetary results: __ Yes __ No **X** N/A

In response to this recommendation, the agency will review IT policies and procedures and make a determination whether updates are needed. Where updates to policies are needed, revised policies will be drafted and submitted for agency clearance. If necessary, interim guidance in the form of a memorandum from the Chief AI Officer will be issued.

Completion or Estimated Completion Date: *Dec 31, 2026*

Recommendation 3: Develop and implement a process to continually review and update USDA's AI inventory.

Agency Response:
Agree with recommendation: **X** Yes __ No
Agree with monetary results: __ Yes __ No **X** N/A

In response to this recommendation, the agency will implement an AI checklist for all IT procurements to identify where AI is being developed or adopted. That checklist will include confirmation that the use case has been entered into the inventory and that a determination of impact has been completed. The Chief AI Officer, or authorized delegate, will approve or deny submissions based on a review of the checklist.

Completion or Estimated Completion Date: June *30, 2026*

Recommendation 4: Develop and implement a process to ensure a risk assessment, ATO determination, and an overall system impact analysis is conducted prior to AI technologies being permitted on the USDA network.

Agency Response:
Agree with recommendation: **X** Yes __ No
Agree with monetary results: __ Yes __ No **X** N/A

In response to this recommendation, the agency will develop a process to review ATO'd systems, or new systems requiring an ATO, for the introduction of artificial intelligence. Where AI is introduced, the Chief AI Officer and the Chief Information Security Officer will adopt a process with steps and timelines for reviewing the ATO and conducting an impact analysis. Where needed, and in the absence of any other risk assessment (e.g. via FedRAMP authorization), a risk assessment will be conducted.

Completion or Estimated Completion Date: *Dec 31, 2026*

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

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