U.S. DEPARTMENT OF HOMELAND SECURITY

OFFICE OF INSPECTOR GENERAL

OIG-25-10

January 30, 2025

FINAL REPORT

DHS Has Taken Steps to Develop and Govern Artificial Intelligence, But More Action is Needed to Ensure Appropriate Use

OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Washington, DC 20528 | www.oig.dhs.gov

January 30, 2025

MEMORANDUM FOR: Randolph Alles
Senior Official Performing the Duties of the Under Secretary
for Management

FROM: Joseph V. Cuffari, Ph.D.
Inspector General

JOSEPH V CUFFARI

Digitally signed by
JOSEPH V CUFFARI
Date: 2025.01.30
14:44:26 -05'00'

SUBJECT: *DHS Has Taken Steps to Develop and Govern Artificial Intelligence, But More Action is Needed to Ensure Appropriate Use*

Attached for your action is our final report, *DHS Has Taken Steps to Develop and Govern Artificial Intelligence, But More Action is Needed to Ensure Appropriate Use*. We incorporated the formal comments provided by your office.

The report contains 20 recommendations aimed at improving DHS' governance of artificial intelligence. Your office concurred with 20 recommendations. Based on information provided in your response to the draft report, we consider recommendations 1 through 7 and 9 through 20 open and resolved. Based on information provided in your response to the draft report recommendation 8 is closed and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions and of the disposition of any monetary amounts.

Please send your response or closure request to OIGAuditsFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please contact me with any questions, or your staff may contact Kristen Bernard, Deputy Inspector General for Audits, at (202) 981-6000.

Attachment

DHS OIG HIGHLIGHTS

DHS Has Taken Steps to Develop and Govern Artificial Intelligence, But More Action is Needed to Ensure Appropriate Use

January 30, 2025

Why We Did This Audit

Federal agencies use AI to increase mission capabilities and improve services provided to the public. From 2022 to 2023, DHS reported increased use of AI to complete its critical mission of securing the homeland. Although AI provides significant opportunities, it also introduces new challenges and risks that must be appropriately governed to ensure AI is used responsibly and ethically. We conducted this audit to determine the extent to which DHS has developed and implemented governance for the management of AI.

What We Recommend

We made a total of 20 recommendations to DHS, comprised of 7 identical recommendations to DHS components, to improve the Department's ability to govern and oversee AI to ensure ethical and trustworthy use of the technology.

For Further Information:
Contact our Office of Public Affairs at (202) 981-6000, or email us at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.

What We Found

The Department of Homeland Security has taken steps to develop guidance and establish oversight for artificial intelligence (AI) use, but more action is needed to ensure DHS governs and manages AI use appropriately. DHS issued AI-specific guidance, appointed a Chief AI Officer, and established multiple working groups and its AI Task Force to help guide the Department's AI efforts. However, more action is needed to ensure DHS has appropriate governance for responsible and secure use of AI.

Additionally, DHS established an AI strategy to guide enterprise-wide AI goals and objectives, but it did not effectively execute the strategy because it did not develop an implementation plan. Further, DHS did not have adequate governance processes to monitor AI compliance with privacy and civil rights and civil liberties requirements due to resource challenges.

Lastly, DHS developed processes to track and report its use of AI to the public, as required, but the processes did not identify and track some of the data needed to report the Department's AI use cases. DHS also had limited evidence to demonstrate why it considered its AI use consistent with Federal requirements, as DHS and its components did not have a formalized process to identify, review, and validate data included in the Department's mandated AI reporting.

Without appropriate, ongoing governance of its AI, DHS faces an increased risk that its AI efforts will infringe upon the safety and rights of the American people.

DHS Response

DHS concurred with all 20 recommendations.

Table of Contents

Abbreviations

AI	Artificial Intelligence
AIPWG	Artificial Intelligence Policy Working Group
AITF	Artificial Intelligence Task Force
CAIO	Chief Artificial Intelligence Officer
CBP	U.S. Customs and Border Protection
CISA	Cybersecurity and Infrastructure Security Agency
CISOD	Chief Information Security Officer Directorate
CRCL	Office for Civil Rights and Civil Liberties
CTOD	Chief Technology Officer Directorate
ECD	Estimated Completion Date
EO	Executive Order
FC	Face Capture
FEMA	Federal Emergency Management Agency
FR	Face Recognition
Gen AI	Generative Artificial Intelligence
ICE	U.S. Immigration and Customs Enforcement
IT	Information Technology
NIST	National Institute of Standards and Technology
OCFO PA&E	Office of the Chief Financial Officer Program Analysis and Evaluation
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
PACT	Office of Privacy, Access, Civil Liberties, and Transparency
PCR	Privacy Compliance Review
PRIV	DHS Privacy Office
ROB	Rules of Behavior
TSA	Transportation Security Administration
USCIS	U.S. Citizenship and Immigration Services

Background

Artificial intelligence (AI) is widely considered one of the most powerful and impactful technologies currently available. The term ‘‘artificial intelligence’’ refers to a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments.[1] Within the Federal Government, agencies have been increasingly investing in AI and using its capacities to increase mission capabilities, improve services provided to the public, and help the United States maintain its technology advantage over adversaries. In 2023, Federal agencies publicly reported that over 700 AI investments were being planned or actively used to improve government services (also known as “use cases”).[2] Notable AI disciplines and categories used across the Federal Government to support mission operations include:

- Machine Learning: A type of AI in which machines receive inputs in the form of training data and generate rules to produce outputs.

- Generative AI (Gen AI): A type of AI that broadly describes machine learning systems capable of generating text, images, code, or other types of content. This category includes Commercial Gen AI, which represents technology or products owned by private companies and available for purchase and use from the public marketplace.

- Face Recognition (FR) and Face Capture (FC): FR technology compares an individual’s facial features to available images or video for verification or identification, and FC is any combination of face detection and collection technologies used to identify and extract a face from an image or video.

For agencies with diverse and complex mission requirements such as the Department of Homeland Security, AI presents significant opportunities to improve organizational performance and efficiency. In response to the potential benefits of AI, DHS components have implemented AI by automating mission support processes and activities. Table 1 lists the seven components within our audit scope and notable examples of how they currently use AI to support their mission.

[1] 15 U.S.C. § 9401(3).

[2] 2023 Consolidated AI Use Case Inventory from AI.gov as of September 1, 2023.

Table 1. DHS Components' Mission and AI Use

Component	*Mission*	*AI Use*
Cybersecurity and Infrastructure Security Agency (CISA)	National Coordinator for critical infrastructure security and resilience and acts as the operational lead for Federal cybersecurity.	Analyze large groups of cybersecurity data to identify potential threats.
Federal Emergency Management Agency (FEMA)	Aids communities before, during, and after disasters.	Identify structural damage caused by disasters.
Transportation Security Administration (TSA)	Ensures freedom of movement for people and commerce.	Expedite the processing and entry of airport passengers.
U.S. Citizenship and Immigration Services (USCIS)	Oversees lawful immigration into the United States.	Expedite the processing and review of immigration and naturalization documents.
U.S. Customs and Border Protection (CBP)	Counters terrorism, secures borders, and facilitates lawful trade and entry into the United States.	Verify travelers' identities by comparing live images with existing photos of travel documents.
U.S. Immigration and Customs Enforcement (ICE)	Enforces immigration laws and conducts criminal investigations to mitigate transnational threats, facilitates lawful trade and immigration, and safeguards the American people.	Assist personnel in conducting investigations, such as those identifying perpetrators engaging in child exploitation offenses.
United States Secret Service (Secret Service)	Ensures the safety and security of critical stakeholders and oversees significant national events.	Secret Service is performing research and development to determine viability of AI implementation for mission purposes.

Source: Generated by DHS Office of Inspector General based on DHS' public AI inventory

DHS continues to research and explore how AI can be used to increase innovation and capabilities for key mission areas. In fact, in 2024 DHS established three lines of effort[3] intended to leverage AI to advance DHS' mission, promote nation-wide AI safety and security, and lead AI advancement through strong, cohesive partnerships. For example, DHS reported that FEMA intends to use Gen AI to help underserved communities and local governments develop hazard mitigation strategies to build community resilience. Additionally, DHS reported that USCIS and ICE plan to use large language models[4] to train immigration officers and enhance investigative processes used to combat human trafficking and child exploitation.

Although AI provides significant opportunities to increase the effectiveness and efficiency of mission operations, it poses unique risks due to its collection of sensitive data. Also, it may be susceptible to harmful bias and erosion of privacy. To address these challenges and ensure AI is safe, secure, and trustworthy, Federal requirements have been established through Executive Orders (EOs)[5] and the Office of Management and Budget (OMB)[6] for Federal agencies to ensure that processes are in place to strengthen AI governance, advance responsible AI innovation, and manage risks from the use of AI. The U.S. Government Accountability Office (GAO) and the National Institute of Standards and Technology (NIST) released AI frameworks[7] that offer practices to help agencies ensure the responsible use of AI. Further, to assess whether Federal agencies are in alignment with Federal requirements and best practices, the GAO has performed oversight work[8] on agencies' AI capabilities.

In response, Federal agencies have begun establishing roles and responsibilities for AI governance. Within DHS, the DHS Chief AI Officer (CAIO) serves as the Department's senior AI official, helping to drive innovation and guide strategy for the Department's AI efforts, and the DHS Chief Technology Officer Directorate (CTOD) provides support and oversight of the Department's AI priorities and initiatives. DHS also relies on offices with specific areas of expertise to help govern the Department's efforts for AI. For example, DHS Privacy Office (PRIV) and DHS Office for Civil Rights and Civil Liberties (CRCL) help to ensure the responsible

[3] *DHS Artificial Intelligence Roadmap 2024,* March 17, 2024.

[4] A type of machine learning model that can perform natural language processing tasks such as generating and classifying text, answering questions, and translating text.

[5] EOs regarding AI use include *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, EO 14110, October 30, 2023, and *Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government*, EO 13960, December 3, 2020.

[6] OMB published guidance to govern AI use through its memorandum, *Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence*, OMB Memorandum 24-10, March 28, 2024.

[7] *Artificial Intelligence Risk Management Framework*, NIST AI 100-1, January 2023, and *Artificial Intelligence, An Accountability Framework for Federal Agencies and Other Entities*, GAO 21-519SP, June 2021.

[8] *Artificial Intelligence, Agencies Have Begun Implementation but Need to Complete Key Requirements*, GAO-24-105980, December 2023, *and Artificial Intelligence, Fully Implementing Key Practices Could Help DHS Ensure Responsible Use for Cybersecurity*, GAO-24-106246, February 2024.

and ethical use of AI by providing oversight of the Department's AI compliance with existing laws and DHS requirements in their respective areas of responsibility. DHS components have started to assign AI governance roles to specific offices and individuals. Recognizing the need to be transparent, DHS has also developed mechanisms to help foster public trust. DHS reports its AI use cases to the public[9] and shares details regarding its recent AI efforts, AI-related guidance, and planned AI initiatives on a public-facing departmental website dedicated to AI.

We conducted this audit to determine the extent to which DHS has developed and implemented governance for the management of AI.

Results of Audit

DHS has taken steps to develop guidance and establish oversight for AI use, but more action is needed to ensure DHS governs and manages AI use appropriately. DHS issued AI-specific guidance, appointed a Chief AI Officer, and established multiple working groups and its AI Task Force to help guide the Department's AI efforts. However, more action is needed to ensure DHS has appropriate governance for responsible and secure use of AI.

Additionally, DHS established an AI strategy to guide enterprise-wide AI goals and objectives, but it did not effectively execute the strategy because it did not develop an implementation plan. Further, DHS did not have adequate governance processes to monitor AI compliance with privacy and civil rights and civil liberties requirements due to resource challenges.

Lastly, DHS developed processes to track and report its use of AI to the public, as required, but the processes did not identify and track some of the data needed to report the Department's AI use cases. DHS also had limited evidence to demonstrate why it considered its AI use consistent with Federal requirements, as DHS and its components did not have a formalized process to identify, review, and validate data included in the Department's mandated AI reporting.

Without appropriate, ongoing governance of its AI, DHS faces an increased risk that its AI efforts will infringe upon the safety and rights of the American people.

[9] Some AI, such as that used in military or law enforcement operations, is considered sensitive. To protect the mission, DHS may not share details of these use cases with the public.

DHS Has Established AI Governance Roles and Responsibilities to Manage its Adoption of AI to Support Its Mission Across the Department

DHS took action to assign roles and responsibilities for AI governance to manage its adoption of AI for mission capabilities. DHS reported broad AI use across its components for specific mission processes. To manage these use cases, DHS appointed a CAIO, established departmental AI working groups, initiated the Artificial Intelligence Task Force (AITF), and developed governance processes for specific AI capabilities to better leverage the technology across the homeland security enterprise and meet Federal and DHS policy requirements.

DHS Made Plans and Adopted AI to Advance and Support the Department's Mission

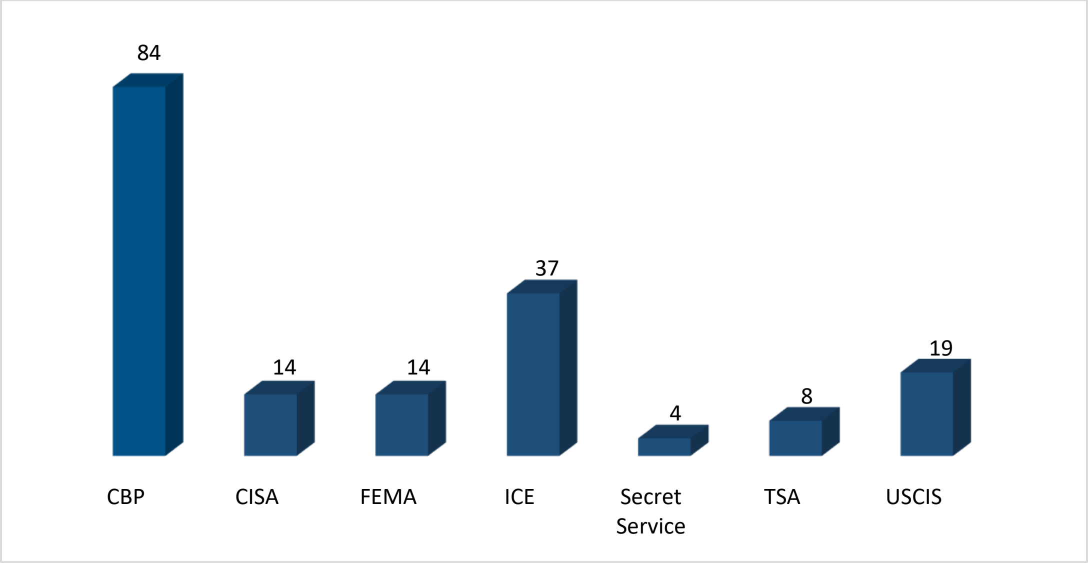
DHS implemented AI capabilities (including AI systems, Gen AI, and FR and FC technologies) to support its critical mission of securing the homeland. According to DHS' internal reporting, DHS had approximately 350[10] AI use cases in various stages of development from planning to initiation[11] to implementation[12] across the Department. Of the 350 estimated AI use cases, we identified 180 that were managed by the seven components within the scope of our audit, as shown in Figure 1.

[10] This data includes AI use cases that are not shared with the public (i.e., sensitive use cases) and AI use cases that were outside the scope of our audit.

[11] Initiation is a NIST term relating to the identification of the need for a system and documentation of the system's purpose and high-level requirements in the System Development Life Cycle.

[12] Implementation is a NIST term relating to the deployment of a system in the System Development Life Cycle. *Contingency Planning Guide for Federal Information Systems*, NIST Special Publication 800-34 Revision 1, May 2010.

Figure 1. Total Number of AI Use Cases by DHS Component as of January 2024[13]



Source: DHS OIG analysis of DHS-provided data

All seven components we evaluated had either begun to explore AI or were already using AI to support mission capabilities. As indicated above, CBP reported 84 use cases to support its mission operations, including at ports of entry to record arrivals to and from the United States and to detect items of interest. ICE reported 37 use cases, including AI used to collect data from known perpetrators of crimes, while FEMA reported 14 AI use cases, including AI to increase the efficiency of disaster response operations and hazard mitigation planning. Overall, DHS reported it anticipated that components' use of AI would improve mission performance and service delivery.

DHS Established Roles and Responsibilities to Support AI Governance and Adoption

DHS appointed a CAIO to promote AI innovation and safety across the Department and advise the Department's leadership on AI-related topics. DHS proactively appointed the CAIO in September 2023, 8 months before Federal requirements[14] mandated this action. DHS' CAIO sets strategic priorities for AI deployment across the Department and, on behalf of the Secretary, coordinates AI-related efforts in partnership with DHS offices and components. DHS reported the CAIO has also worked with congressional committees to share information

[13] This figure includes AI use cases that are not shared with the public (i.e., sensitive) and only includes the components we examined as part of the audit scope.
[14] *Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence*, OMB Memorandum 24-10, March 28, 2024.

about how DHS intends to use AI in the future and how DHS plans to combat AI risks. Additionally, DHS established a department-wide AI task force and two working groups to support AI efforts:

- The DHS Secretary established the AITF in April 2023[15] to address emerging AI advancements. The AITF led initiatives to increase AI collaboration and adoption, such as a DHS AI Pilot Program and various AI-related educational opportunities. In 2023, DHS' AI Pilot Program granted funding for three pilot projects aimed at advancing AI for key mission processes managed by USCIS, ICE, and FEMA and raised awareness of adversarial AI threats by publishing a series of studies on preparedness for DHS stakeholders.

- DHS initiated the Responsible Use Group[16] in June 2023 to provide guidance, risk assessment, mitigation strategies, and oversight for projects championed by the AITF. The group's efforts include working to advance the equitable use of AI and building a common vocabulary around responsible AI use across DHS.

- DHS required the establishment of the AI Policy Working Group (AIPWG) in August 2023 to effect policy change as outlined in DHS requirements.[17] The AIPWG collaborates across the Department to assess and support the development of policies, procedures, and processes needed to support AI.

DHS Established Governance for Commercial Generative AI

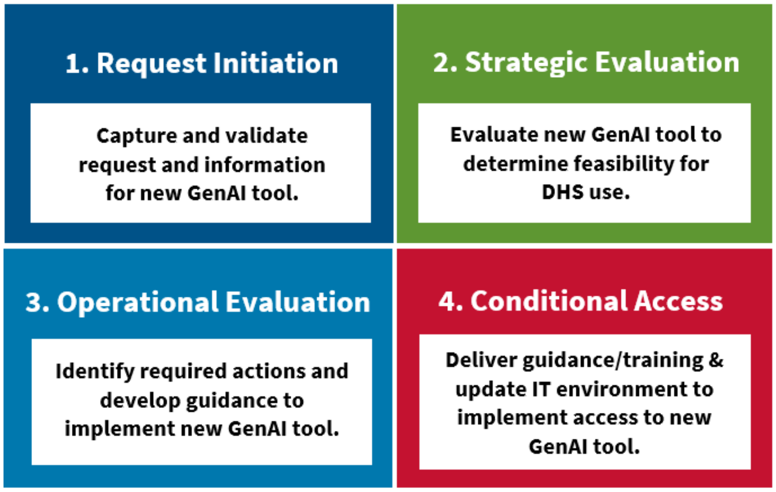
DHS took steps to leverage potential benefits and provide governance of commercial Gen AI. Commercial Gen AI tools are growing in popularity because they may be used to generate new, novel content, such as audio, code, images, text, and videos. DHS reported[18] that, when used appropriately, commercial Gen AI may enhance existing programs and improve departmental business functions, such as conducting research, developing draft materials, and preparing for meetings and events.

To take advantage of commercial Gen AI's benefits and provide appropriate governance for its use, DHS implemented a process to conditionally approve specific commercial Gen AI tools for use across the Department. DHS' conditional approval process for commercial Gen AI included reviews to evaluate accuracy, security practices, supply chain concerns, privacy

[15] *Establishment of a DHS Artificial Intelligence Task Force*, DHS AITF Memorandum, April 20, 2023.
[16] DHS' Responsible Use Group is chaired by the Officer for Civil Rights and Civil Liberties within the AITF.
[17] *Acquisition and Use of AI and Machine Learning Technologies by DHS Components*, DHS Policy Statement 139-06, August 8, 2023.
[18] *Privacy Impact Assessment for the Use of Conditionally Approved Commercial Generative Artificial Intelligence Tools,* November 19, 2023.

and civil liberties safeguards, and the source of data used to train the AI tool. Figure 2 depicts DHS' conditional approval process for commercial Gen AI tools.

Figure 2. DHS' Conditional Approval Process for Commercial Gen AI Tools



1. Request Initiation

Capture and validate request and information for new GenAI tool.

2. Strategic Evaluation

Evaluate new GenAI tool to determine feasibility for DHS use.

3. Operational Evaluation

Identify required actions and develop guidance to implement new GenAI tool.

4. Conditional Access

Deliver guidance/training & update IT environment to implement access to new GenAI tool.

Source: Generated by DHS OIG based on *DHS Privacy Impact Assessment for Use of Conditionally Approved Commercial Generative Artificial Intelligence Tools*

DHS has formally tracked its conditionally approved commercial Gen AI tools. As of November 2023, DHS conditionally approved four commercial Gen AI tools to advance mission applications of AI across the Department. DHS components may use DHS' conditional approval process or develop component-specific processes to approve commercial Gen AI tools.

In addition to establishing the conditional approval process, DHS established the Gen AI Rules of Behavior (ROB) and Gen AI training to address the risk of potential privacy, civil rights, civil liberties, and legal issues associated with Gen AI tools. All DHS personnel are required to sign the ROB and complete the training before they can use conditionally approved commercial Gen AI tools. The ROB includes information on the acceptable use of commercial Gen AI tools, data protection and retention, accountability for use of products derived from Gen AI tools, and incident reporting. DHS Gen AI training provides information regarding AI, machine learning, and Gen AI, as well as subsets of Gen AI such as large language models. It also covers additional topics such as DHS' current commercial Gen AI use, responsible use, and risks associated with the technology. DHS advised that more than 3,000 personnel across the Department attended the training as of February 2024.

DHS Established Governance for Face Recognition and Face Capture Technologies

DHS implemented AI such as FR and FC technologies to support mission requirements including law enforcement and border security. DHS components currently use FR and FC technologies to verify international travelers' identities and documentation by matching travelers' photos with previously captured images from component databases. As of January 2024, DHS reported 44 FR and FC technologies in various stages of development across the Department.

DHS reported that FR and FC technologies are inherently privacy sensitive. Therefore, it is essential that DHS use FR and FC technologies in a manner that safeguards privacy and civil rights and civil liberties. To support governance and oversight of the Department's FR and FC technologies, DHS implemented a FR and FC policy[19] that provides requirements, roles, and responsibilities for safe and appropriate use. The DHS Office of the Chief Information Officer established a cross-functional oversight team[20] to conduct a 120-day review of existing FR and FC technologies, including those that were in development, to determine if the technologies complied with laws, regulations, and DHS' FR and FC policy. As part of its review, DHS' oversight team verified privacy compliance and civil liberties documentation, confirmed adherence to existing performance metrics, and reviewed approval documentation. In April 2024, DHS CTOD issued a Letter of Technical Assessment[21] outlining the findings and recommendations of the review as well as the actions DHS planned to take to address the conclusions of the review.

DHS Developed an Enterprise-Wide AI Strategy and Subsequent Policies, but Additional Action Is Needed to Implement Strategic Objectives

Consistent with Federal guidance and best practices,[22] DHS developed AI-specific strategic planning and policies. DHS publicly released its AI strategy and three AI policies to guide the Department's AI efforts in 2020 and 2023, respectively. However, DHS has not yet executed all its strategic goals and acknowledged that further departmental guidance is needed to appropriately govern AI.

[19] *Use of Face Recognition and Face Capture Technologies*, DHS Directive 026-11, September 11, 2023.
[20] The FR and FC oversight team included representatives from the Office of the Chief Information Officer, PRIV, Office of the Chief Information Security Officer, Science and Technology Directorate, CRCL, and Policy.
[21] *Letter of Technical Assessment: Review of Existing Uses of Face Recognition and Face Capture Technologies at DHS,* April 3, 2024.
[22] *Preparation, Submission, and Execution of the Budget*, OMB Circular No. A–11, August 11, 2023.

DHS Developed an Enterprise AI Strategy but Has Not Yet Executed its Objectives

In 2020, DHS developed its *Artificial Intelligence Strategy*[23] to help the Department take a proactive role in the ongoing national developments on AI. The strategy was intended to provide a unified and deliberate approach to the Department's AI use and investments. As part of the strategy, DHS established five goals to guide the Department's AI efforts. Within each of the five AI goals, DHS established specific objectives that serve as the Department's foundation for integrating AI into its mission in a responsible and trustworthy manner while mitigating risks associated with AI across the homeland security enterprise. Table 2 depicts the five goals outlined in the strategy and notable strategic objectives.

[23] *DHS Artificial Intelligence Strategy*, December 3, 2020.

Table 2. 2020 DHS AI Strategy Goals and Objectives

Strategy Goal	Strategy Objectives
Goal 1 Assess Potential Impact of AI on the Homeland Security Enterprise	• Develop Knowledge of Technical Applications of AI • Identify Opportunities for AI Use • Identify Critical Applications and Impact of AI on U.S. Critical Infrastructure
Goal 2 Invest in DHS AI Capabilities	• Survey Existing Capabilities for Security and Storage Capacity • Develop Plans to Upgrade Department Infrastructure • Evaluate and Invest in AI Research and Development
Goal 3 Mitigate AI Risks to the Department and to the Homeland	• Develop a Process for Continual Evaluation of AI Risks • Produce and Release Public AI Data Use Guidance • Formalize AI Governance Processes at DHS
Goal 4 Develop a DHS AI Workforce	• Identify Current AI Expertise and Gaps Across DHS • Identify External AI Training Courses and Make Available to Workforce • Partner with Academic and Private Sector to Develop a Public/Private Sector Fellowship Program
Goal 5 Improve Public Trust and Engagement	• Develop Strategic Communications Plan to Support Communication to the Public on AI • Establish a Framework for Releasing AI System Information for Public Comment • Communicate Identified AI-Related Risks

Source: Generated by DHS OIG based on DHS' AI Strategy

Although DHS' AI Strategy provided a unified approach to help support safe and secure AI use throughout the Department, DHS did not fully execute the strategy. Specifically, DHS did not develop an implementation plan, as required,[24] to harmonize and prioritize the AI planning, programming, budget, training, and execution activities outlined in the strategy. Nor did DHS annually assess and report progress in executing the strategy to the Secretary, as required.[25] We were therefore unable to determine if certain DHS efforts used to support the strategy

[24] *DHS Artificial Intelligence Strategy*, December 3, 2020.
[25] *DHS Artificial Intelligence Strategy*, December 3, 2020.

met the intent of the requirements. For example, the strategy required that DHS conduct a survey to identify personnel with AI experience. Although DHS provided a list of personnel who fulfilled AI-related tasks across the Department, we could not determine whether DHS had performed a comprehensive survey to identify personnel. DHS advised that many of the actionable tasks required by the strategy were not previously completed and would not be executed unless they were included in an update to the strategy. To keep pace with recent AI advancements across the Department and remain consistent with new Federal criteria[26] DHS released an AI Roadmap[27] in March 2024. We did not evaluate whether this roadmap was intended to replace or update the initial DHS AI Strategy from 2020 because it was released after we concluded audit fieldwork.

DHS officials provided conflicting information on why the 2020 AI Strategy was not fully executed. Some officials believed the strategy had been rescinded, but DHS did not provide documentation of the decision to discontinue the use of the strategy. The DHS Office of Strategy, Policy, and Plans, which was tasked with developing the implementation plan and producing annual reports, did not develop an implementation plan or produce annual reports because it believed that a different office would typically be assigned the responsibility of executing strategies internally within DHS. Although the strategy was developed to help guide DHS and its components' early AI efforts, some components reported that the strategy was not impactful for operations.

DHS Made Progress in Issuing AI Guidance

The Fiscal Year 2023 National Defense Authorization Act[28] required that DHS issue policies and procedures related to the acquisition and use of AI, the risks and impacts of AI, and privacy and civil liberties considerations for AI. DHS made progress in meeting this requirement and acknowledged that policy and other guidance would be needed to ensuring mission-appropriate, responsible, and rights-protecting use of AI at DHS. In 2023, DHS issued three AI-specific policies to help ensure AI is used ethically and responsibly:

1. *DHS Policy Statement 139-06*, *Acquisition and Use of AI and Machine Learning Technologies by DHS Components*, August 8, 2023. This policy statement was the first AI-specific policy DHS released to guide the Department's safe and responsible use of AI. The policy statement outlined actions that DHS and its

[26] *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, EO 14110, October 30, 2023.
[27] In the *Artificial Intelligence Roadmap 2024* (March 17, 2024), the Department reported new AI use cases and pilot programs across its various mission areas and provided information on its efforts to partner with other agencies.
[28] *James M. Inhofe National Defense Authorization Act for Fiscal Year 2023*, December 23, 2022.

components must undertake to establish policy and practices governing the acquisition and use of AI/machine learning technologies within the Department.

2. *DHS Directive 026-11*, *Use of Face Recognition and Face Capture Technologies* September 11, 2023. This directive established an enterprise policy for the authorized use of FR and FC technologies to support DHS missions while safeguarding privacy, civil rights, and civil liberties. It also required that DHS review all existing FR and FC technologies and provided criteria against which the technologies will be assessed in the future to ensure rights are safeguarded.

3. *DHS Policy Statement 139-07, Use of Commercial Generative AI Tools*, October 24, 2023. This policy statement was established to guide the appropriate use of commercially available generative AI products by DHS' workforce. It provided interim rules for the technology and developed initial guidance such as the development of an approved list of commercial Gen AI tools.

Although DHS made notable progress in its efforts to develop and issue AI-specific policies, it has not yet completed efforts to ensure the Department has the policies needed to appropriately govern the use of AI. DHS self-identified that the following further actions were needed to address AI policy considerations:

- Assess the need for components to update or revise their existing policies, procedures, and processes for the responsible and ethical use of AI across the Department.
- Develop a directive and instruction to facilitate updates that require formal policy changes to proceed.
- Develop an AI Risk Management Framework to evaluate all use cases early in their life cycle to assess risk across a broad range of considerations.
- Review and update *DHS Policy Directive 4300A, IT System Security Program, Sensitive Systems,* for AI considerations.

DHS has not yet completed its AI policy and guidance efforts because the associated requirements[29] were recently issued and are evolving. Specifically, DHS was still within its planned timeline to complete policy-related tasks when our audit fieldwork ended. According to DHS Policy Statement 139-06, the AIPWG had until August 2024 to create an AI-specific Directive and Instruction. The DHS Chief Information Security Officer's Cybersecurity Policy Working Group plans to complete its review and updates of DHS Policy Directive 4300A by September 30, 2024, and the DHS AIPWG advised it was in the process of identifying and

[29] *Acquisition and Use of AI and Machine Learning Technologies by DHS Components*, DHS Policy Statement 139-06, August 8, 2023.

considering the factors that would need to be addressed in the DHS AI Risk Management Framework.

DHS Faced Challenges in Providing Privacy and Civil Rights and Liberties Oversight of AI

DHS did not have adequate governance processes to monitor the Department's AI for compliance with privacy and civil rights and civil liberty requirements. PRIV and CRCL are responsible for ensuring AI does not erode privacy protections or infringe on existing civil liberties considerations, respectively. Although PRIV and CRCL took steps to implement processes to execute their AI oversight responsibilities, both offices faced resource challenges that prevented them from completing the actions necessary to monitor DHS AI.

DHS Privacy Office Did Not Have a Process to Identify, Prioritize, or Monitor Closure of Privacy Compliance Reviews

PRIV is responsible for ensuring that DHS' use of technologies such as AI sustains and does not erode privacy protections relating to the use, collection, and disclosure of personal information. To fulfill its roles and responsibilities, PRIV supported the Department's broader AI oversight initiatives such as assessing FR and FC technologies[30] and Gen AI[31] for privacy considerations. In support of this mission, PRIV uses the Privacy Compliance Review (PCR) process. PRIV conducts PCRs if required[32] or recommended[33] by a program's privacy compliance documentation[34] and at the discretion of the DHS Chief Privacy Officer. During a PCR, PRIV conducts interviews and analyzes supporting documentation to ensure programs comply with applicable privacy laws and policies and assurances made in privacy compliance documentation such as Privacy Impact Assessments.[35] PCRs may result in recommendations for corrective actions, publicly available reports, or discussions with stakeholders on lessons

[30] From September 2023 through January 2024, DHS offices conducted a review of all existing FR and FC technologies in accordance with *Use of Face Recognition and Face Capture Technologies*, Directive 026-11, September 11, 2023.
[31] DHS' Gen AI Integrated Project Team conducted a review of Gen AI tools for provisional authorized use.
[32] Some PCRs result from requirements set in privacy compliance documentation, such as Privacy Impact Assessments.
[33] Existing privacy documentation such as Privacy Impact Assessments may recommend that a Privacy Compliance Review be completed for specific information technology (IT) tools.
[34] DHS programs develop privacy documentation such as Privacy Impact Assessments, which may contain requirements or recommendations for PCRs to be completed.
[35] A privacy compliance documentation and process that PRIV must follow when an activity involves the planned use of personal identifiable information or may otherwise impact the privacy of individuals as determined by the Chief Privacy Officer according to *Privacy Policy and Compliance*, DHS Directive 047-01-001, July 25, 2011.

learned. According to one of DHS' recently issued AI policies,[36] PRIV has the authority to initiate and conduct PCRs on FR and FC technologies used by the Department.

Although PRIV issued a standard operating procedure[37] to formally document its methodology for completing PCRs, the current process does not have adequate controls to appropriately identify PCRs that are required or recommended by DHS program office privacy documentation. PRIV acknowledged that it did not have a process to track PCRs required or recommended by DHS program documentation. In 2024, PRIV completed an internal review to identify ongoing and incomplete PCRs. PRIV's internal review identified seven required and eight recommended PCRs that were not completed as specified by DHS program documentation, including one AI-related PCR for Generative AI. PRIV's insufficient controls regarding PCRs that are required or recommended increases the risk that PCRs of AI technology will not be completed in the future when needed.

In addition to PCRs required and recommended by DHS program offices, PRIV may conduct PCRs at the discretion of the DHS Chief Privacy Officer. Although discretionary PCRs may be used to further the Department's oversight of DHS program offices' privacy compliance, we determined that PRIV had not conducted any discretionary PCRs, including for AI, since 2020. Also, PRIV did not have a process to identify and prioritize DHS programs that should be subjected to discretionary PCRs. PRIV's internal policies and procedures did not include risk factors or considerations that should be evaluated to determine if discretionary PCRs should be conducted for critical Department technologies such as AI. PRIV acknowledged that it may identify potential discretionary PCRs that should be conducted if an incident or significant privacy event takes place, but it had not developed formal documentation for this process.

PRIV did not monitor and track whether DHS program offices completed recommendations to address PCR findings. Although PRIV required[38] DHS program offices to develop and agree to schedules for implementing PCR recommendations, PRIV did not ensure this process was completed. We found that 18 of the 20 recommendations that PRIV issued to components between June 2015 and June 2019 remained open without evidence of periodic follow-up to monitor recommendation status. PRIV initiated an effort in 2024 to evaluate the status of recommendations and corrective actions.

DHS Privacy Office Faced Resource Challenges

PRIV did not establish formalized processes to track required and recommended PCRs, prioritize discretionary PCRs, or monitor PCR recommendations because it faced significant

[36] *Use of Face Recognition and Face Capture Technologies*, DHS Directive 026-11*,* September 11, 2023.
[37] *Privacy Compliance Review Standard Operating Procedure*, November 2016.
[38] *Privacy Compliance Review Standard Operating Procedure*, November 2016.

resource constraints (i.e., longstanding staffing challenges and competing priorities). PRIV officials advised that the office only had one part-time staff member to perform PCRs until FY 2023 and that it did not have the personnel needed to develop and implement governance controls to identify, track, and prioritize PCRs. Since 2023, PRIV hired at least one new full-time equivalent staff member to support the PCR process. PRIV also explained that additional personnel and training may still be needed to ensure it can perform PCRs as intended. To address this anticipated need, PRIV started evaluating potential training that should be provided to staff who perform PCRs and developed a training proposal for increasing its personnel's skills in performing PCRs.

DHS Office for Civil Rights and Civil Liberties Did Not Have a Formalized Process to Provide Oversight of the Department's AI

DHS policy requires[39] the use of civil rights and civil liberties evaluation methods, including disparate impact analysis where appropriate, to detect impermissible discriminatory treatment resulting from the use of AI in DHS processes and activities. As part of DHS' AI governance structure, CRCL is responsible for providing oversight of the Department's AI to ensure compliance with applicable requirements. Although CRCL supported the Department's broader AI oversight initiatives such as assessing FR and FC technologies[40] and Gen AI[41] for civil rights and civil liberties considerations, it had not yet implemented a process to perform ongoing oversight of the Department's AI.

In 2024, CRCL developed a draft *AI Risk Assessment Framework for Civil Rights and Civil Liberties* to help guide its oversight efforts. However, the framework was not finalized at the time of our audit. Before developing the framework, CRCL officials advised DHS stakeholders of potential concerns regarding the accuracy, accessibility, and transparency of AI. The current contents of CRCL's draft framework would help to address AI-related concerns regarding civil rights and civil liberties. Specifically, the draft framework includes oversight objectives and considerations for evaluating AI risks from relevant sources, such as NIST's AI Risk Management Framework,[42] AI-related EOs, and OMB guidance.

[39] *Acquisition and Use of Artificial Intelligence and Machine Learning Technologies by DHS Components*, DHS Policy Statement 139-06, August 8, 2023.

[40] From September 2023 through January 2024, DHS offices conducted a review of all existing FR and FC technologies in accordance with *Use of Face Recognition and Face Capture Technologies*, Directive 026-11, September 11, 2023.

[41] DHS' Gen AI Integrated Project Team conducted a review of Gen AI tools for provisional authorized use.

[42] *Artificial Intelligence Risk Management Framework*, January 2023.

DHS Office for Civil Rights and Civil Liberties Faced Resource Constraints

CRCL was unable to fully support the evaluation of the increasing number of AI applications across the Department due to resource constraints and the status of DHS' AI oversight efforts. CRCL explained it previously requested additional funding to increase its capacity to perform AI oversight, but further resources would be needed. CRCL was also required to submit a resource request to Congress but had not developed the request at the time of our audit. In addition to resource constraints, CRCL advised DHS was in the early stages of developing formal policy and processes at the time of our testing and had not yet finalized mature documentation for AI tool evaluation. CRCL noted it would further develop its oversight processes once DHS finalized its department-wide AI Risk Management Framework.

DHS Did Not Ensure All Required AI Use Cases and Data Were Reported

DHS is required[43] to report and share all eligible[44] AI use cases with other Government agencies and the public. As part of its reporting, DHS is required to assess existing AI for inconsistencies with Federal requirements. However, DHS' reporting did not contain all the Department's existing eligible AI use cases or evidence to show how it determined the Department's AI was consistent with Federal requirements. This occurred because DHS and its components did not have a formalized process to identify, review, and validate data included in the Department's mandated AI reporting.

DHS Did Not Meet Requirements for Reporting AI to the Public

To comply with EO 13960, *Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government,*[45] DHS reported on its AI use in 2022 and 2023. However, DHS' mandated reporting did not contain all required AI use cases. We determined that 13 AI use cases were reported at least a year after they were required to be reported. Of the 13 AI use cases that were not reported in a timely manner, 9 were initiated before July 2022, but not reported until September 2023, and 4 were initiated before October 2022, but not reported until October 2023.[46] Table 3 lists the DHS AI use cases that were reported late.

[43] *Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government*, EO 13960, December 3, 2020.

[44] Eligible use cases are those that do not meet the exclusion categories outlined by *Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government*, EO 13960, December 3, 2020 (e.g., sensitive, military-related, embedded AI, or research and development efforts).

[45] *Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government*, EO 13960, December 3, 2020.

[46] After our audit fieldwork concluded, DHS provided technical comments to our draft report to further explain the potential root causes of AI use cases not being included in its public reporting as required. However, we were unable to verify the accuracy of this information since our testing was already completed.

Table 3. DHS AI Use Cases Originally Omitted from Mandated Reporting

Component	*AI Use Case Name*
CBP	Automated Item of Interest Detection
CBP	Data and Entity Resolution
USCIS	Identity Match Option Process with Data and Business Intelligence Service Marts
USCIS	Person-Centric Identity Services A-Number Management Model
USCIS	Person-Centric Identity Services Deduplication Model
ICE	Barcode Scanner
ICE	Facial Recognition Service
ICE	Email Analytics
Headquarters CBP, CISA, ICE	RelativityOne
CBP	Port of Entry Risk Assessments
CBP	Traveler Verification Service
TSA	Touchless PreCheck Identity Solution
FEMA	Geospatial Damage Assessments

Source: Generated by DHS OIG based on DHS-provided data

DHS did not ensure that all required data fields (e.g., the dates that specific AI use cases were initiated, developed, and acquired and implemented) were included in the mandated reporting of DHS AI. To support its mandated reporting process, DHS maintained an internal list of all DHS AI use cases to determine which AI use cases should be included in its mandated public reporting. DHS used the internal list to identify AI use cases that were sensitive or otherwise should not be included in the Department's mandated public reporting. We examined DHS' internal AI list and found that it did not contain the data DHS needed to accurately complete its mandated reporting. Although DHS' internal list of AI contained data fields to justify if an AI use case should be excluded from public reporting, these

66 AI use cases on DHS' internal AI inventory were excluded from public reporting without formal justification.

fields were not consistently completed. We identified 66 DHS AI use cases that were not updated with a formal justification to demonstrate why the use cases should be excluded. Given the Department's incomplete internal data, we could not determine whether DHS reported all required AI use cases in accordance with EO 13960.

As part of DHS' mandated reporting of its AI use, the Department must assess existing AI for inconsistencies with EO 13960. To meet this requirement, DHS must attest to whether each of its AI use cases is consistent with the requirements in EO 13960. Although DHS' 2023 mandated reporting of AI concluded that each of its 50 AI use cases[47] were consistent with EO 13960, DHS and its components did not have evidence of the data or assessments used to make these determinations. DHS CTOD attempted to help components assess their use cases for mandated reporting by providing a checklist of items to be evaluated to identify inconsistences with EO 13960. However, most components primarily used the checklist for reference and did not collect documentation to complete or support their assessments.

DHS Faced Challenges in Identifying and Validating AI Data for Public Reporting

DHS did not report all eligible AI use cases and required data because its components did not have consistent processes to appropriately identify, track, and assess eligible AI use cases. Components relied on data calls and reviews of existing IT system inventories to identify and track which AI use cases to share with DHS CTOD for inclusion in the Department's mandated public reporting. Yet components did not formalize or standardize these processes to ensure AI-related data was complete, accurate, and consistent. Several components advised of plans to enhance their processes to identify and track AI use cases to support oversight efforts and the Department's mandated reporting requirements. For example, in FY 2024, the CBP Commissioner established an initiative to enhance CBP's identification and tracking of AI use cases, and CISA developed a goal to increase its tracking of AI use cases in its AI Roadmap released in November 2023.[48]

In addition to facing challenges in receiving adequate data from components, DHS CTOD relied on manual processes to validate the AI data components submitted for inclusion in mandated reporting. When DHS CTOD completed the Department's first mandated public reporting in 2022, it acknowledged that it assembled the report based on component responses to a data call and that it did not take additional steps to ensure component responses included all required AI use cases. In 2023, DHS started using an application to support the identification, tracking, and review of AI use cases that should be included in mandated reporting. However, DHS did not have formalized procedures for inputting, tracking, and validating information in the application. DHS advised it plans to formalize

[47] The 50 AI use cases were publicly reported in DHS' 2023 Public Facing Inventory.
[48] *CISA Roadmap for Artificial Intelligence,* November 2023.

these procedures, but this effort has not yet been completed because processes may continue to change and requirements for mandated reporting are still evolving.

Conclusion

Without appropriate, ongoing governance of its AI, DHS faces an increased risk that the technology will be used in a manner that is not trustworthy, safe, ethical, or transparent to the public. AI poses significant risks of unintended release of sensitive information and bias, which could affect the privacy and civil rights and civil liberties of individuals. DHS cannot ensure that AI does not erode privacy and civil rights protections until its oversight offices have controls in place to adequately perform oversight of AI. Further, DHS may not maintain the public's trust if it does not consistently provide up-to-date and accurate information on how it uses AI. Many of the AI technologies DHS uses interact with and collect information from the public. For this reason, it is imperative that DHS communicate how AI technologies will be used, the types of risks they present, and how the Department aims to mitigate risks.

Recommendations

Recommendation 1: We recommend that the DHS Artificial Intelligence Task Force, in coordination with appropriate stakeholders, evaluate DHS' 2020 Artificial Intelligence Strategy and finalize any updates that it determines are needed.

Recommendation 2: We recommend that the DHS Artificial Intelligence Policy Working Group complete its ongoing efforts to assess and document the need for components to update or revise their existing policies, procedures, and processes for the responsible and ethical use of artificial intelligence.

Recommendation 3: We recommend that the DHS Artificial Intelligence Policy Working Group complete its ongoing efforts to develop a directive and instruction to facilitate updates that require formal policy changes to proceed.

Recommendation 4: We recommend that the DHS Artificial Intelligence Policy Working Group complete its ongoing efforts to develop an Artificial Intelligence Risk Management Framework.

Recommendation 5: We recommend that the DHS Chief Information Security Officer complete its review of and update DHS Policy Directive 4300A for artificial intelligence considerations.

Recommendation 6: We recommend that the DHS Privacy Office evaluate the personnel and training resources of oversight staff to determine additional resources and training required to meet artificial intelligence oversight requirements and act as needed based on the results of the evaluation.

Recommendation 7: We recommend that the DHS Privacy Office update the Privacy Compliance Review process to formally track required Privacy Compliance Reviews.

Recommendation 8: We recommend that DHS Privacy Office document its methodology to include the considerations that should be formally evaluated for prioritizing programs that may be subject to discretionary PCRs as provided in its standard operating procedure.

Recommendation 9: We recommend that the DHS Privacy Office develop and implement a formalized process for tracking and closing Privacy Compliance Review recommendations.

Recommendation 10: We recommend that the DHS Office for Civil Rights and Civil Liberties evaluate the personnel resources needed to meet civil rights and civil liberties oversight requirements and act as needed based on the results of the evaluation.

Recommendation 11: We recommend that the DHS Office for Civil Rights and Civil Liberties finalize its Artificial Intelligence Risk Management Framework or implement an alternative process to provide oversight of DHS artificial intelligence's compliance with civil rights and civil liberties considerations.

Recommendation 12: We recommend that CBP implement DHS' enterprise process to identify, assess, and track AI use cases or implement a component specific process to identify, assess, and document artificial intelligence use cases and the associated data required for the Department's mandated public reporting of artificial intelligence.

Recommendation 13: We recommend that CISA implement DHS' enterprise process to identify, assess, and track AI use cases or implement a component specific process to identify, assess, and document artificial intelligence use cases and the associated data required for the Department's mandated public reporting of artificial intelligence.

Recommendation 14: We recommend that FEMA implement DHS' enterprise process to identify, assess, and track AI use cases or implement a component specific process to identify, assess, and document artificial intelligence use cases and the associated data required for the Department's mandated public reporting of artificial intelligence.

Recommendation 15: We recommend that ICE implement DHS' enterprise process to identify, assess, and track AI use cases or implement a component specific process to identify, assess, and document artificial intelligence use cases and the associated data required for the Department's mandated public reporting of artificial intelligence.

Recommendation 16: We recommend that TSA implement DHS' enterprise process to identify, assess, and track AI use cases or implement a component specific process to identify, assess, and document artificial intelligence use cases and the associated data required for the Department's mandated public reporting of artificial intelligence.

Recommendation 17: We recommend that USCIS implement DHS' enterprise process to identify, assess, and track AI use cases or implement a component specific process to identify, assess, and document artificial intelligence use cases and the associated data required for the Department's mandated public reporting of artificial intelligence.

Recommendation 18: We recommend that Secret Service implement DHS' enterprise process to identify, assess, and track AI use cases or implement a component specific process to identify, assess, and document artificial intelligence use cases and the associated data required for the Department's mandated public reporting of artificial intelligence.

Recommendation 19: We recommend that the DHS Chief Technology Officer Directorate develop and implement a formalized process to review, validate, and approve data that components provide for DHS' mandated reporting of the Department's artificial intelligence use.

Recommendation 20: We recommend that the DHS Chief Technology Officer Directorate develop and implement procedures to ensure components provide accurate and complete data for DHS' mandated reporting of the Department's artificial intelligence use.

Management Comments and OIG Analysis

DHS provided management comments on a draft of this report. Appendix B contains a copy of the Department's comments in their entirety. We also received technical comments from DHS on the draft report under separate cover and revised the report as appropriate. DHS concurred with all 20 of our recommendations. We consider recommendations 1-7 and 9-20 open and resolved. Recommendation 8 is closed and resolved. A summary of the Department's response and our analysis follows.

DHS Response to Recommendation 1: Concur. The DHS 2020 Artificial Intelligence Strategy will be replaced by the mandated AI strategy aligning with requirements in M-24-10. In replacing the older strategy, DHS positions itself to leverage AI more effectively to safeguard the Nation while also promoting ethical practices, enhancing public trust, and ensuring compliance with current laws and regulations. Estimated Completion Date (ECD): April 30, 2025.

OIG Analysis: DHS' actions are responsive to the recommendation. This recommendation will remain open and resolved until DHS provides documentation of the finalized AI strategy aligning with M-24-10.

DHS Response to Recommendation 2: Concur. The AIPWG finished coordination with components to assess existing AI policies, procedures, and processes, and determined that a DHS directive and instruction are necessary to drive comprehensive, coordinated policy changes. These efforts began in November 2023 and the draft of the directive for internal review was created in June 2024. The forthcoming directive and instruction will document needed updates and revisions to existing policies, procedures, and processes and provide guidance to components regarding responsible use of AI. ECD: January 31, 2025.

OIG Analysis: DHS' actions are responsive to the recommendation. This recommendation will remain open and resolved until DHS provides: (1) documentation of its assessment of existing policies, procedures, and processes for AI considerations; and (2) the finalized directive and instruction to drive AI-related policy updates.

DHS Response to Recommendation 3: Concur. The AIPWG will complete a directive and instruction that will provide guidance to components on the responsible use of AI and facilitate updates that require formal policy changes to proceed. The directive and instruction will outline a new risk management framework for DHS' use of AI and targeted strategies for acquisition of AI. ECD: January 31, 2025.

OIG Analysis: DHS' actions are responsive to the recommendation. This recommendation will remain open and resolved until DHS provides documentation of its finalized directive and instruction to drive AI-related policy updates.

DHS Response to Recommendation 4: Concur. The forthcoming directive and instruction being developed by the AIPWG will also outline a DHS AI Risk Management Framework. Once complete, CTOD will coordinate with components to ensure the ongoing implementation of the framework to keep pace with rapid advancements in AI. ECD: January 31, 2025.

OIG Analysis: DHS' actions are response to the recommendation. This recommendation will remain open and resolved until DHS provides documentation of the finalized AI Risk Management Framework.

DHS Response to Recommendation 5: Concur. DHS Office of the Chief Information Officer (OCIO) and Chief Information Security Officer Directorate (CISOD), in coordination with the OCIO CISOD Policy team, placed initial focus regarding AI efforts on the completion of updates to the AI System Security Guide, as well as the interim Rules of Behavior. OCIO

CISOD will continue its review of 4300A policy in FY 2025 to identify any potential policy areas that may need updates to address AI. In addition, the OCIO CISOD Policy team will continue working with AI stakeholders to address potential policy updates that may be needed. ECD: December 31, 2025.

OIG Analysis: DHS' actions are responsive to the recommendation. This recommendation will remain open and resolved until DHS provides: (1) supporting evidence of its review of 4300A for AI-related policy updates; and (2) documentation of finalized updates to 4300A made as part of its review (as applicable).

DHS Response to Recommendation 6: Concur. At the request of PRIV, the DHS Office of the Chief Financial Officer (OCFO) Program Analysis and Evaluation (PA&E) conducted a staffing assessment with Privacy Office leadership to ensure that staffing resources are aligned with organizational priorities, workloads, and budget constraints. PRIV actively participated in all aspects of the comprehensive evaluation to identify any existing gaps and establish a benchmark for developing and/or requesting funding to address these gaps. The evaluation determined that PRIV, through the Privacy Oversight Team, currently has the necessary resources in place to effectively oversee and manage the training and oversight requirements of AI technologies. The Privacy Oversight Team is equipped to address the challenges that may arise and ensure compliance with regulatory frameworks and will ensure PRIV remains agile and responsive as AI continues to evolve, leveraging existing resources to maintain robust training, oversight, and accountability.

OIG Analysis: DHS' actions are responsive to the recommendation. The recommendation will remain open and resolved until DHS provides supporting evidence of OCFO PA&E's staffing assessment of PRIV, including the results of the evaluation that the Privacy Oversight Team has the necessary resources to manage training and oversight requirements for AI.

DHS Response to Recommendation 7: Concur. PRIV already tracks required PCRs by maintaining a spreadsheet tracking PCRs required but not yet performed, as well as the completed PCRs' recommendation implementation statuses. However, tracking of required PCRs will be formalized through an upcoming update to the Privacy Compliance Tracking System. This update will enable PRIV to track timelines and completion of major milestones and associated activities throughout the PCR process. ECD: November 28, 2025.

OIG Analysis: DHS' actions are responsive to the recommendation. The recommendation will remain open and resolved until DHS provides: (1) evidence supporting the update of the Privacy Compliance Tracking System; (2) evidence supporting the functionality of the system update to formally track PCR timelines and completion of major milestones.

DHS Response to Recommendation 8: Concur. On August 19, 2024, PRIV provided us documentation of the Privacy Compliance Review Prioritization model, which identifies risk levels from low to high based on the type of activity involved and the source of the PCR requirement. For example, incidents or events demonstrating a broad and/or ongoing risk will rank higher in priority than a recommendation in privacy compliance documentation that a program or activity may be a candidate for a PCR at some future date. Subsequently, on September 12, 2024, PRIV provided us with the decision memorandum, which officially approved the adoption of the model.

OIG Analysis: DHS provided documentation showing its corrective actions in response to recommendation 8. Specifically, PRIV provided the finalized PCR prioritization model, which outlines the risk factors that influence the initiation of PCRs. For example, the model contains privacy risks from low to high that are considered for initiating PCRs. The Privacy Office also provided a memorandum of the formal approval and adoption of the prioritization model by PRIV. Recommendation 8 is resolved and closed.

DHS Response to Recommendation 9: Concur. PRIV currently tracks open PCR recommendations using “quad charts” and is developing a standard operating procedure for PCR follow-up that will formalize PRIV’s process for tracking and closing recommendations. Further, as previously mentioned, PRIV will also formalize tracking through the Privacy Compliance Tracking System in a future system update. ECD: November 28, 2025.

OIG Analysis: DHS’ actions are responsive to the recommendation. This recommendation will remain open and resolved until DHS provides: (1) the finalized standard operating procedure for PCR follow-up that includes processes for tracking and closing recommendations; and (2) supporting evidence for PCR follow-up capabilities within the Privacy Compliance Tracking System.

DHS Response to Recommendation 10: Concur. CRCL evaluated resource needs to provide policy advice, conduct oversight activities, and support training requirements associated with Department’s adoption of AI. Specifically, from March 2024 to June 2024, CRCL participated in an evaluation led by OCFO PA&E, which assessed DHS’ AI priorities, identified the Department’s capability gaps, and presented funding options that close or reduce identified gaps. As part of the evaluation, an assessment of CRCL’s resources, gap analysis, and funding options were taken into consideration for the Department’s FY26 budget request so that CRCL could effectively support the Department’s AI activities. CRCL provided documentation of these efforts on December 4, 2024.

OIG Analysis: DHS' actions are responsive to the recommendation. The recommendation will remain open and resolved until DHS provides supporting evidence of the evaluation results and recommended actions that should be taken by CRCL (as applicable).

DHS Response to Recommendation 11: Concur. An initial draft of a civil rights and civil liberties AI Risk Management Framework was first available in early 2024. Principles from the initial framework have informed the development of individual rights protections in the draft DHS Enterprise Risk Management Framework, which is under development. CRCL will produce a final version of a civil rights and civil liberties risk management framework informed by CAIO-led process for identifying, mitigating, and managing risks to safety-impacting and rights-impacting AI. ECD: March 31, 2025.

OIG Analysis: DHS' actions are responsive to the recommendation. This recommendation will remain open and resolved until DHS provides documentation of its finalized civil rights and civil liberties risk management framework for AI.

DHS Response to Recommendation 12: Concur. CBP is currently working with the AIPWG and the DHS OCIO's AI Policy and Enterprise Governance Lead to ensure CBP compliance with OMB M-24-10. Since 2020, CBP's AI Office provided annual input to the required DHS AI Use Case Inventory Data Call and is currently working across the agency in anticipation of receiving the 2024 request, with a planned submission by December 2024. CBP is also documenting the agency review and recommendations for AI use case safety-impacting and/or rights-impacting determinations, which will be submitted for DHS CAIO signature. ECD: January 31, 2025.

OIG Analysis: CBP's actions are responsive to the recommendation. This recommendation will remain open and resolved until CBP provides evidence of its formal implementation of DHS' AI Use Case Inventory process or evidence of its component-specific process to identify, assess, and document AI use cases.

DHS Response to Recommendation 13: Concur. CISA's OCIO and the Office of Privacy, Access, Civil Liberties, and Transparency (PACT) co-lead CISA's efforts to responsibly use AI in support of the agency's mission. The OCIO and PACT team is finalizing a new internal governance process to identify, assess, and track AI use cases, which is anticipated to be in effect by January 2025. The CISA PACT team will also continue to collaborate with the DHS CAIO staff to ensure CISA use cases are properly documented and submitted in a timely fashion for DHS Headquarter review and final determinations on whether any of CISA's use cases are safety-impacting and/or rights-impacting AI. ECD: January 31, 2025.

OIG Analysis: CISA's actions are responsive to the recommendation. This recommendation will remain open and resolved until CISA provides evidence of its formal implementation of DHS' AI Use Case Inventory process or evidence of its component specific process to identify, assess, and document artificial intelligence use cases.

DHS Response to Recommendation 14: Concur. On July 2, 2024, the FEMA Administrator established the Artificial Intelligence Enterprise Steering Group to define FEMA's approach regarding the development and deployment of AI solutions, lead efforts to accelerate the employment of AI, and establish appropriate governance to ensure responsible use. To enable governance, FEMA OCIO, in coordination with the FEMA Office of Policy and Program Analysis, developed the AI Use Case automated tool in September 2024 to identify, assess, and track FEMA use cases. This tool facilitates the approval, processing, and reporting to AI use cases in compliance with OMB and DHS guidance.

OIG Analysis: FEMA's actions are responsive to the recommendation. This recommendation will remain open and resolved until FEMA provides evidence of its formal implementation of DHS' AI Use Case Inventory process or evidence of its component-specific process to identify, assess, and document artificial intelligence use cases.

DHS Response to Recommendation 15: Concur. ICE OCIO uses DHS' processes since direction was established on February 1, 2022. Accordingly, ICE OCIO uses tools provided by DHS to maintain the DHS AI Use Case inventory, consistent with DHS processes to identify, assess, and document AI use cases and associated required data. On October 22, 2024, ICE provided OIG with supporting documentation of adopting DHS' enterprise process.

OIG Analysis: ICE's actions are responsive to the recommendation. The recommendation will remain open and resolved until ICE provides supporting evidence of its formal implementation of DHS' AI Use Case Inventory process, or formal implementation of a component-specific process to identify, assess, and document artificial intelligence use cases.

DHS Response to Recommendation 16: Concur. TSA's CAIO is actively involved in DHS working groups such as the AIPWG and Responsible Use Group. TSA is fully prepared to adopt DHS policies and AI use case reporting standards as each are finalized. In addition, TSA's CAIO is currently evaluating and building governance processes and procedures for internal stakeholder engagement as well as AI use case identification, assessment, and documentation in conjunction with CRCL, PRIV, and TSA's legal counsel. ECD: September 30, 2025.

OIG Analysis: TSA's actions are responsive to the recommendation. The recommendation will remain open and resolved until TSA provides evidence of its formal implementation of DHS' AI Use Case Inventory process or evidence of its component-specific process to identify, assess, and document artificial intelligence use cases.

DHS Response to Recommendation 17: Concur. USCIS adopted DHS' enterprise process to identify, assess, track, and update agency AI use cases based on reporting guidance issued by DHS beginning in summer 2022. In January 2024, the USCIS Director designated the USCIS Chief Technology Officer to serve as the Component Senior AI Officer, who established guidance on the requirements to identify and track current and future use cases and the USCIS AI Governance Board. The governance board will be integral to the development of processes to identify, review, approve, and monitor the responsible use of AI tools across USCIS. Additionally, USCIS, in coordination with the DHS OCIO is developing a formalized process for the review of existing and newly proposed AI use cases, pursuant to OMB 24-M-10, which will be completed by December 31, 2024. ECD: March 31, 2025.

OIG Analysis: USCIS' actions are responsive to the recommendation. The recommendation will remain open and resolved until USCIS provides evidence of its formal implementation of DHS' AI Use Case Inventory process or evidence of its component-specific process to identify, assess, and document artificial intelligence use cases.

DHS Response to Recommendation 18: Concur. In October 2024, the Secret Service adopted and actively utilized the DHS enterprise process to assess and track AI use cases in accordance with OMB M-24-10. Evidence of this adoption is reflected in the DHS AI use case reporting system, Mobius, in which Secret Service currently had three active AI use cases in progress. Furthermore, on July 16, 2024, the Secret Service developed an internal process to feed the DHS mandated process, "AI Community of Interest Cross Functional Workflow."

OIG Analysis: The Secret Service's actions are responsive to the recommendation. The recommendation will remain open and resolved until Secret Service provides supporting evidence of its adoption of DHS' inventory process (once finalized) and official approval documentation for its internal workflow (e.g., signed memorandum).

DHS Response to Recommendation 19: Concur. On October 25, 2024, the OCIO CTOD updated DHS' "AI Use Case Inventory instructions," which is used as part of the FY 2024 AI Use Case Inventory process. This guidance includes a process to review, validate, and approve component submissions to DHS' Use Case Inventory data call. The DHS 2024 Use Case Inventory, created in accordance with the new DHS guidance, will be completed by December 31, 2024. ECD: January 31, 2025.

OIG Analysis: DHS' actions are responsive to the recommendation. The recommendation will remain open and resolved until DHS provides supporting evidence for its formalized process to review, validate, and approve data that components provide for DHS' mandated reporting of AI.

DHS Response to Recommendation 20: Concur. As previously noted, the OCIO CTOD developed DHS AI Use Case Inventory instructions to be used during the FY 2024 AI Use Case Inventory process on October 25, 2024. These instructions include a process to validate the accuracy of component submissions to DHS' Use Case Inventory data call. The DHS 2024 Use Case Inventory, created in accordance with new DHS guidance, will be completed by December 31, 2024. ECD: January 31, 2025.

OIG Analysis: DHS' actions are responsive to the recommendation. The recommendation will remain open and resolved until DHS provides procedures to ensure components provide accurate and complete data for DHS' mandated reporting of AI.

Appendix A:
Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Pub. L. No. 107−296) by amendment to the *Inspector General Act of 1978.*

We conducted this audit to determine the extent to which DHS has developed and implemented governance for the management of artificial intelligence. The audit included DHS Management Directorate offices responsible for providing oversight of AI and operational and support components that use or would benefit from AI to execute their missions. As part of this audit, we evaluated challenges, best practices, and lessons learned from current and planned AI investments and focused on departmental and component strategies, governance processes, implementation standards, internal controls, and information system controls for managing AI. However, because our review was limited to these internal control components and underlying principles, it may not have disclosed all internal control deficiencies that may have existed at the time of this audit.

To conduct this audit, we gathered documentation related to AI governance and implementation, including Federal, departmental, and component criteria, and evidence of departmental and component AI implementation and governance. We met with DHS Office of the Chief Information Officer; DHS Privacy Office; CRCL; DHS Science and Technology Directorate; DHS Office of Strategy, Policy, and Plans; DHS components, the AIPWG, and the AITF. We used the information gathered to assess the adequacy of DHS' governance and oversight controls to support AI use across the Department and the effectiveness of DHS' management oversight of components' efforts to acquire, develop, and maintain AI. We also used this information to assess the adequacy of DHS' efforts to develop and disseminate guidance to secure AI technologies across the homeland security enterprise; the sufficiency of departmental AI strategies and standards; and the effectiveness of the DHS Management Directorate's processes for collaborating with components on AI standards, best practices, and departmental requirements. Although we did not use statistical analysis for this audit, we did test the reliability of computer-processed data and determined the data was sufficiently reliable for audit purposes.

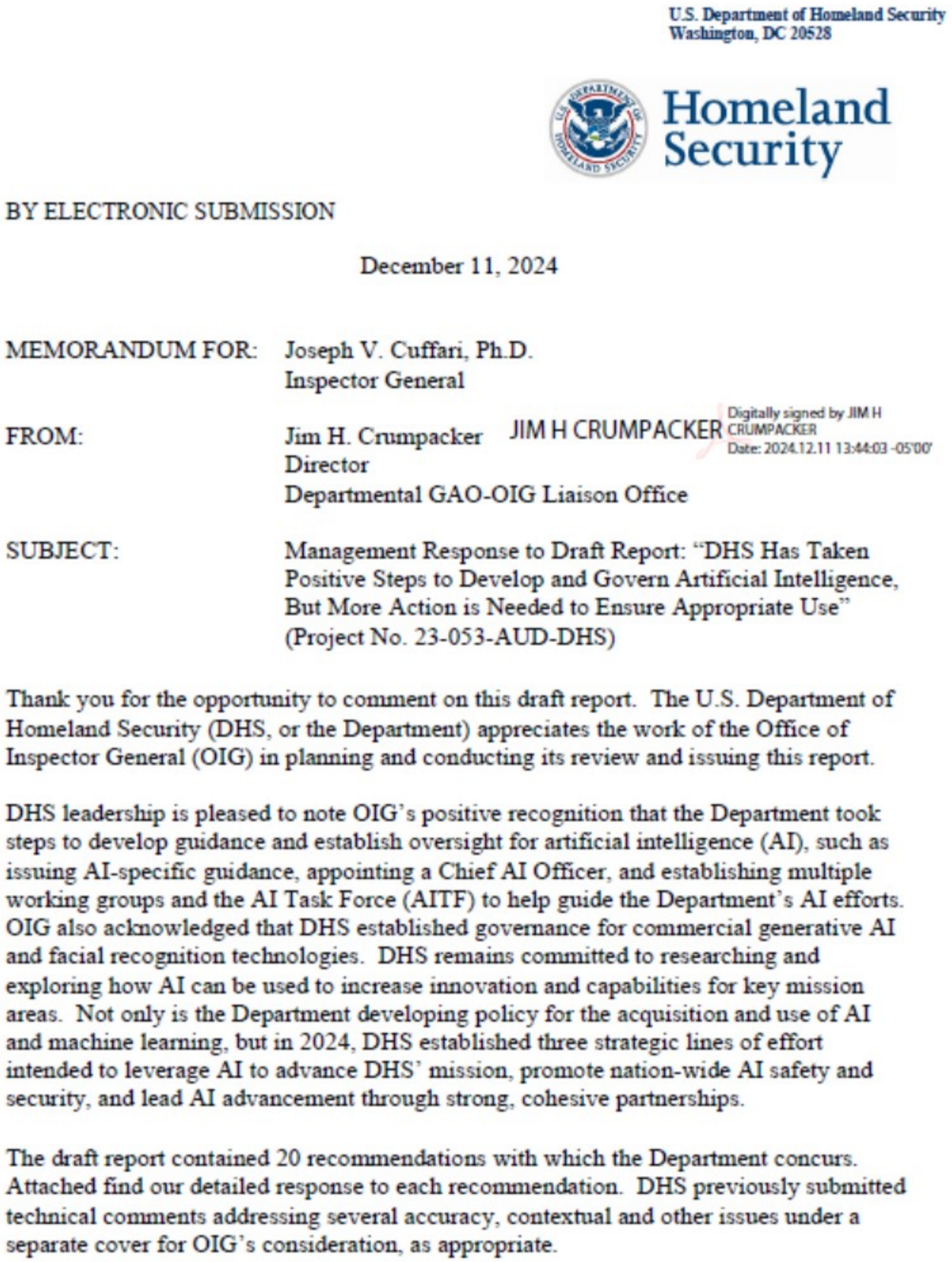
We also obtained an understanding of operational and support component processes for developing and managing AI. Specifically, for each selected component, we assessed whether AI plans, strategies, standards, and procedures have been developed and if component guidance aligns with departmental policy. We also assessed the extent that each of the major operational components has implemented (or plans to implement) AI and if components have best practices and lessons learned on potential shortcomings and barriers in achieving their AI goals.

We conducted this audit from September 2023 through March 2024 pursuant to the Inspector General Act of 1978, 5 U.S.C. §§ 401–424, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

DHS OIG's Access to DHS Information

During this audit, DHS provided timely responses to our requests for information and did not delay or deny access to information we requested.

Appendix B:
DHS Comments on the Draft



U.S. Department of Homeland Security
Washington, DC 20528

Homeland
Security

BY ELECTRONIC SUBMISSION

December 11, 2024

MEMORANDUM FOR: Joseph V. Cuffari, Ph.D.
Inspector General

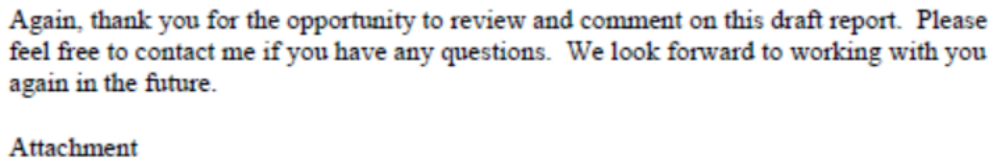
FROM: Jim H. Crumpacker JIM H CRUMPACKER Digitally signed by JIM H CRUMPACKER Date: 2024.12.11 13:44:03 -05'00'
Director
Departmental GAO-OIG Liaison Office

SUBJECT: Management Response to Draft Report: "DHS Has Taken Positive Steps to Develop and Govern Artificial Intelligence, But More Action is Needed to Ensure Appropriate Use"
(Project No. 23-053-AUD-DHS)

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS, or the Department) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

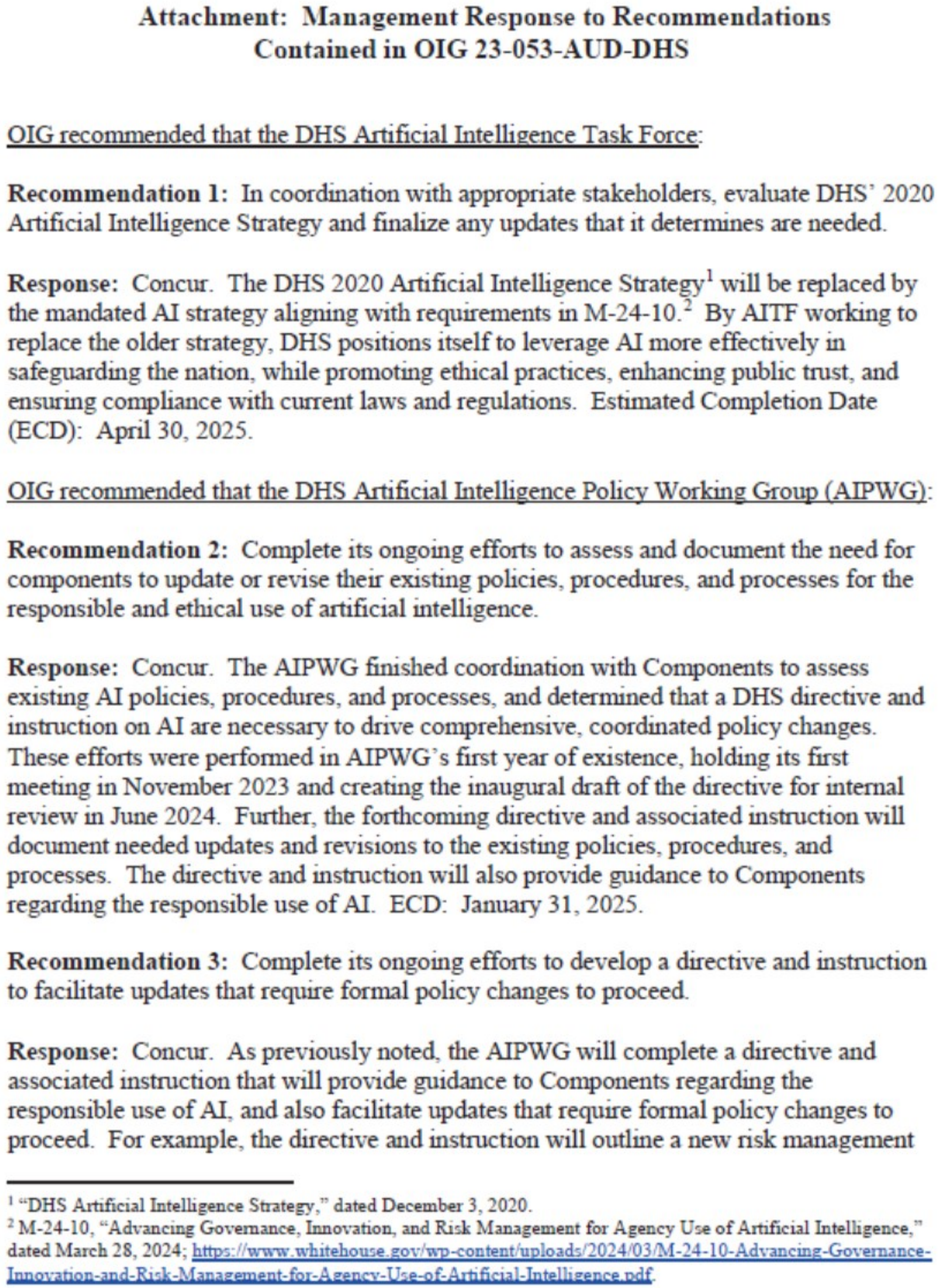
DHS leadership is pleased to note OIG's positive recognition that the Department took steps to develop guidance and establish oversight for artificial intelligence (AI), such as issuing AI-specific guidance, appointing a Chief AI Officer, and establishing multiple working groups and the AI Task Force (AITF) to help guide the Department's AI efforts. OIG also acknowledged that DHS established governance for commercial generative AI and facial recognition technologies. DHS remains committed to researching and exploring how AI can be used to increase innovation and capabilities for key mission areas. Not only is the Department developing policy for the acquisition and use of AI and machine learning, but in 2024, DHS established three strategic lines of effort intended to leverage AI to advance DHS' mission, promote nation-wide AI safety and security, and lead AI advancement through strong, cohesive partnerships.

The draft report contained 20 recommendations with which the Department concurs. Attached find our detailed response to each recommendation. DHS previously submitted technical comments addressing several accuracy, contextual and other issues under a separate cover for OIG's consideration, as appropriate.



Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Attachment



Attachment: Management Response to Recommendations Contained in OIG 23-053-AUD-DHS

OIG recommended that the DHS Artificial Intelligence Task Force:

Recommendation 1: In coordination with appropriate stakeholders, evaluate DHS' 2020 Artificial Intelligence Strategy and finalize any updates that it determines are needed.

Response: Concur. The DHS 2020 Artificial Intelligence Strategy[1] will be replaced by the mandated AI strategy aligning with requirements in M-24-10.[2] By AITF working to replace the older strategy, DHS positions itself to leverage AI more effectively in safeguarding the nation, while promoting ethical practices, enhancing public trust, and ensuring compliance with current laws and regulations. Estimated Completion Date (ECD): April 30, 2025.

OIG recommended that the DHS Artificial Intelligence Policy Working Group (AIPWG):

Recommendation 2: Complete its ongoing efforts to assess and document the need for components to update or revise their existing policies, procedures, and processes for the responsible and ethical use of artificial intelligence.

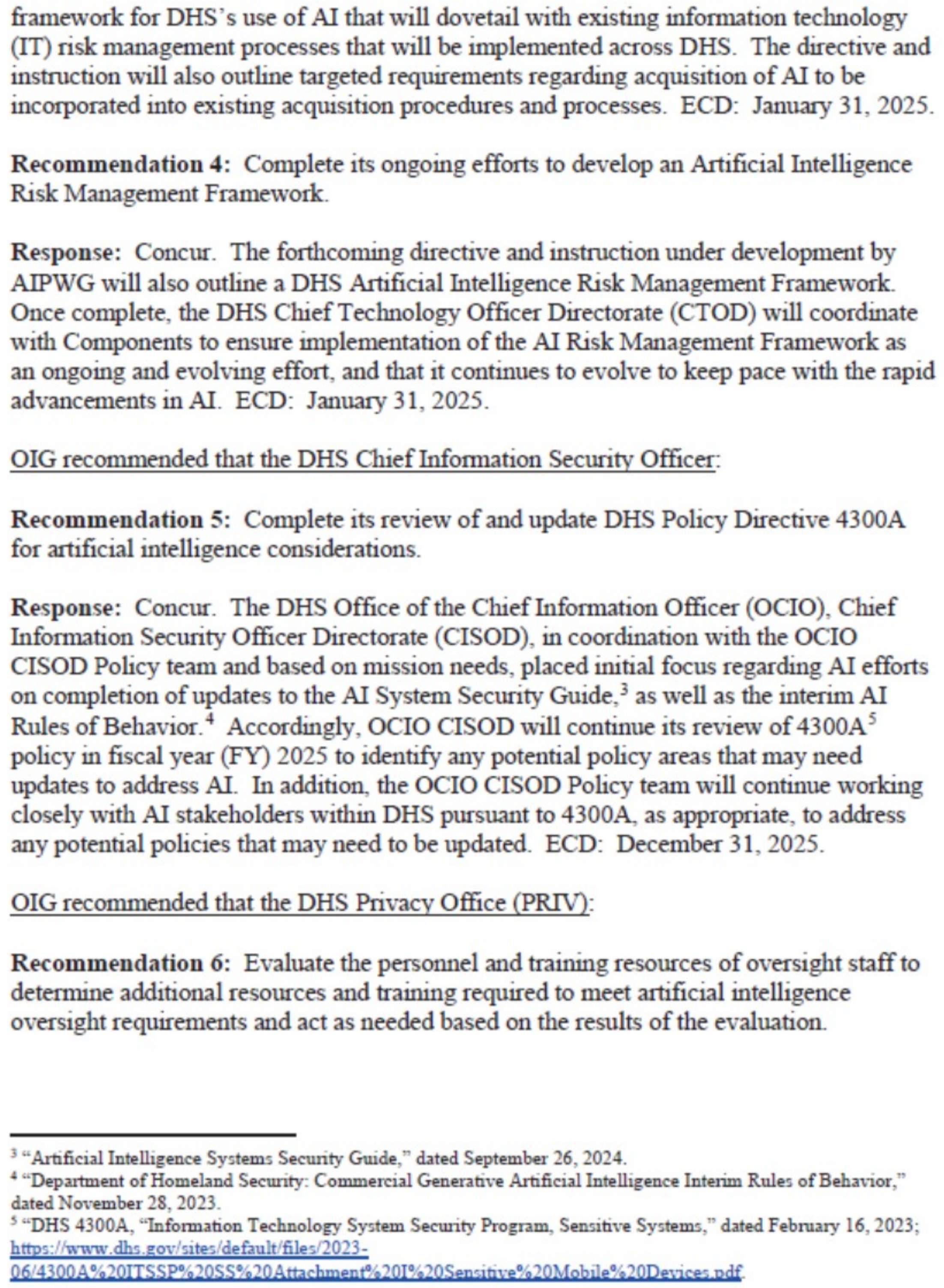
Response: Concur. The AIPWG finished coordination with Components to assess existing AI policies, procedures, and processes, and determined that a DHS directive and instruction on AI are necessary to drive comprehensive, coordinated policy changes. These efforts were performed in AIPWG's first year of existence, holding its first meeting in November 2023 and creating the inaugural draft of the directive for internal review in June 2024. Further, the forthcoming directive and associated instruction will document needed updates and revisions to the existing policies, procedures, and processes. The directive and instruction will also provide guidance to Components regarding the responsible use of AI. ECD: January 31, 2025.

Recommendation 3: Complete its ongoing efforts to develop a directive and instruction to facilitate updates that require formal policy changes to proceed.

Response: Concur. As previously noted, the AIPWG will complete a directive and associated instruction that will provide guidance to Components regarding the responsible use of AI, and also facilitate updates that require formal policy changes to proceed. For example, the directive and instruction will outline a new risk management

[1] "DHS Artificial Intelligence Strategy," dated December 3, 2020.

[2] M-24-10, "Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence," dated March 28, 2024; https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf.



framework for DHS's use of AI that will dovetail with existing information technology (IT) risk management processes that will be implemented across DHS. The directive and instruction will also outline targeted requirements regarding acquisition of AI to be incorporated into existing acquisition procedures and processes. ECD: January 31, 2025.

Recommendation 4: Complete its ongoing efforts to develop an Artificial Intelligence Risk Management Framework.

Response: Concur. The forthcoming directive and instruction under development by AIPWG will also outline a DHS Artificial Intelligence Risk Management Framework. Once complete, the DHS Chief Technology Officer Directorate (CTOD) will coordinate with Components to ensure implementation of the AI Risk Management Framework as an ongoing and evolving effort, and that it continues to evolve to keep pace with the rapid advancements in AI. ECD: January 31, 2025.

<u>OIG recommended that the DHS Chief Information Security Officer</u>:

Recommendation 5: Complete its review of and update DHS Policy Directive 4300A for artificial intelligence considerations.

Response: Concur. The DHS Office of the Chief Information Officer (OCIO), Chief Information Security Officer Directorate (CISOD), in coordination with the OCIO CISOD Policy team and based on mission needs, placed initial focus regarding AI efforts on completion of updates to the AI System Security Guide,[3] as well as the interim AI Rules of Behavior.[4] Accordingly, OCIO CISOD will continue its review of 4300A[5] policy in fiscal year (FY) 2025 to identify any potential policy areas that may need updates to address AI. In addition, the OCIO CISOD Policy team will continue working closely with AI stakeholders within DHS pursuant to 4300A, as appropriate, to address any potential policies that may need to be updated. ECD: December 31, 2025.

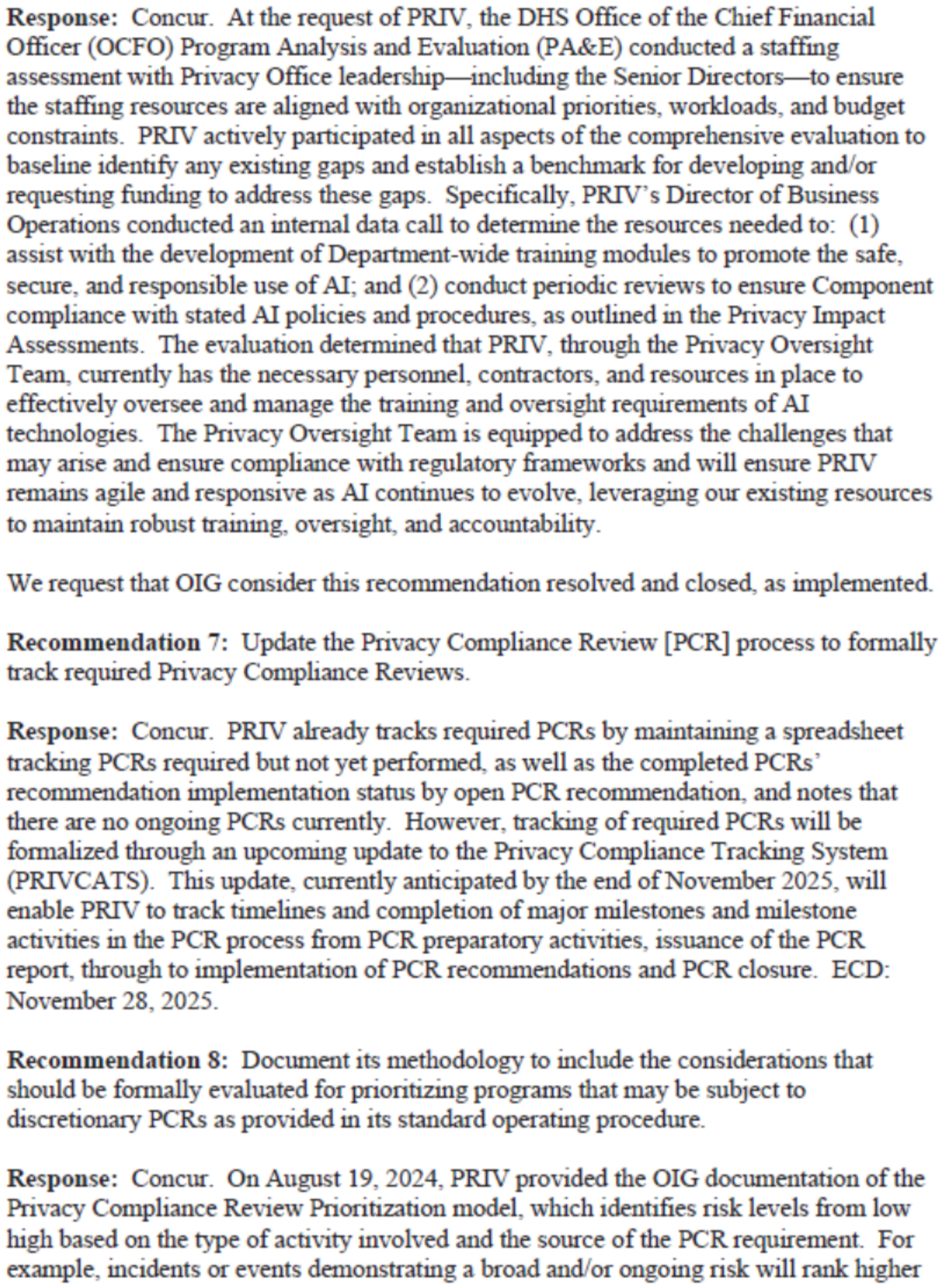
<u>OIG recommended that the DHS Privacy Office (PRIV)</u>:

Recommendation 6: Evaluate the personnel and training resources of oversight staff to determine additional resources and training required to meet artificial intelligence oversight requirements and act as needed based on the results of the evaluation.

[3] "Artificial Intelligence Systems Security Guide," dated September 26, 2024.

[4] "Department of Homeland Security: Commercial Generative Artificial Intelligence Interim Rules of Behavior," dated November 28, 2023.

[5] "DHS 4300A, "Information Technology System Security Program, Sensitive Systems," dated February 16, 2023; https://www.dhs.gov/sites/default/files/2023-06/4300A%20ITSSP%20SS%20Attachment%20I%20Sensitive%20Mobile%20Devices.pdf.



Response: Concur. At the request of PRIV, the DHS Office of the Chief Financial Officer (OCFO) Program Analysis and Evaluation (PA&E) conducted a staffing assessment with Privacy Office leadership—including the Senior Directors—to ensure the staffing resources are aligned with organizational priorities, workloads, and budget constraints. PRIV actively participated in all aspects of the comprehensive evaluation to baseline identify any existing gaps and establish a benchmark for developing and/or requesting funding to address these gaps. Specifically, PRIV's Director of Business Operations conducted an internal data call to determine the resources needed to: (1) assist with the development of Department-wide training modules to promote the safe, secure, and responsible use of AI; and (2) conduct periodic reviews to ensure Component compliance with stated AI policies and procedures, as outlined in the Privacy Impact Assessments. The evaluation determined that PRIV, through the Privacy Oversight Team, currently has the necessary personnel, contractors, and resources in place to effectively oversee and manage the training and oversight requirements of AI technologies. The Privacy Oversight Team is equipped to address the challenges that may arise and ensure compliance with regulatory frameworks and will ensure PRIV remains agile and responsive as AI continues to evolve, leveraging our existing resources to maintain robust training, oversight, and accountability.

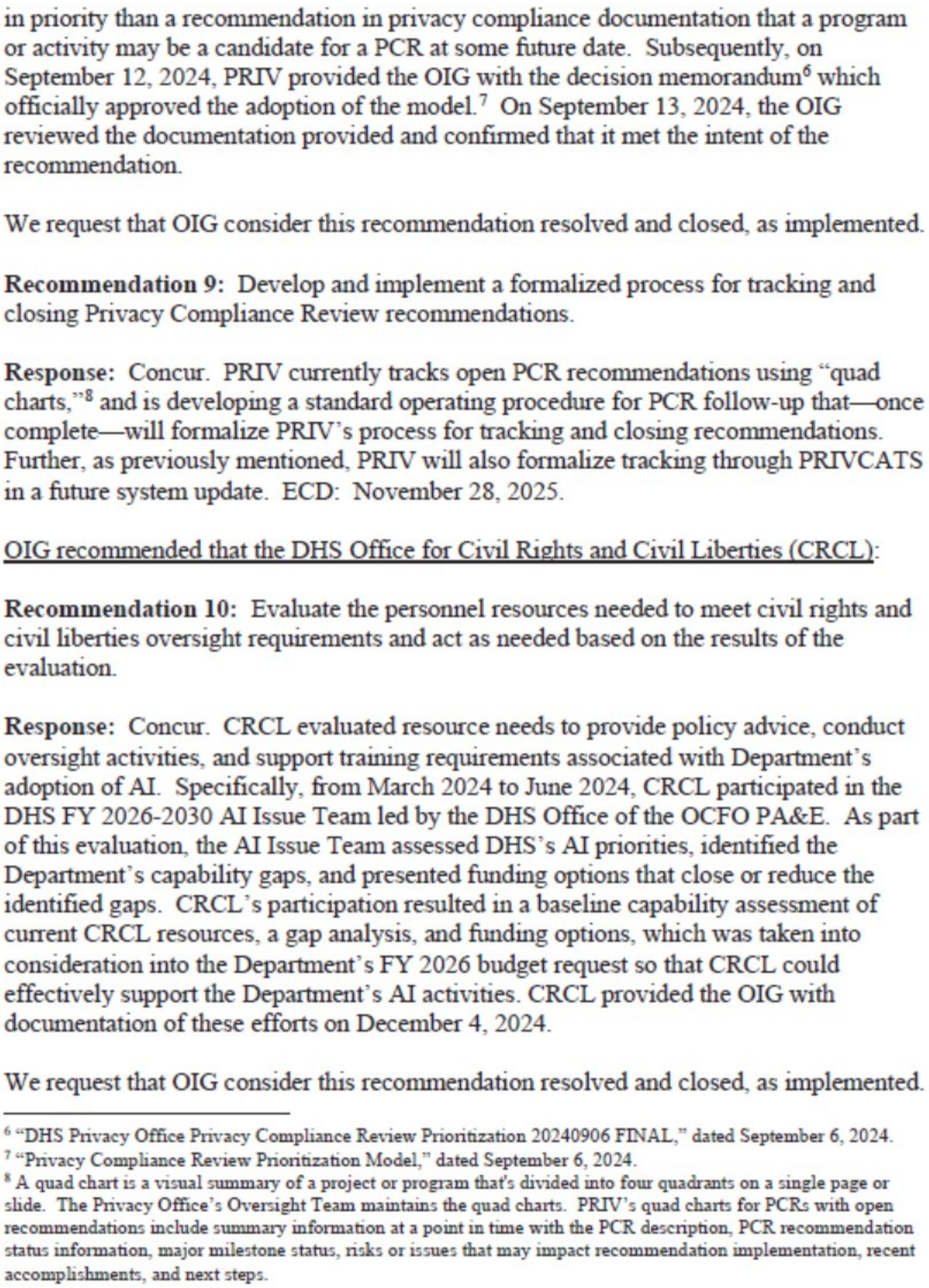
We request that OIG consider this recommendation resolved and closed, as implemented.

Recommendation 7: Update the Privacy Compliance Review [PCR] process to formally track required Privacy Compliance Reviews.

Response: Concur. PRIV already tracks required PCRs by maintaining a spreadsheet tracking PCRs required but not yet performed, as well as the completed PCRs' recommendation implementation status by open PCR recommendation, and notes that there are no ongoing PCRs currently. However, tracking of required PCRs will be formalized through an upcoming update to the Privacy Compliance Tracking System (PRIVCATS). This update, currently anticipated by the end of November 2025, will enable PRIV to track timelines and completion of major milestones and milestone activities in the PCR process from PCR preparatory activities, issuance of the PCR report, through to implementation of PCR recommendations and PCR closure. ECD: November 28, 2025.

Recommendation 8: Document its methodology to include the considerations that should be formally evaluated for prioritizing programs that may be subject to discretionary PCRs as provided in its standard operating procedure.

Response: Concur. On August 19, 2024, PRIV provided the OIG documentation of the Privacy Compliance Review Prioritization model, which identifies risk levels from low high based on the type of activity involved and the source of the PCR requirement. For example, incidents or events demonstrating a broad and/or ongoing risk will rank higher



in priority than a recommendation in privacy compliance documentation that a program or activity may be a candidate for a PCR at some future date. Subsequently, on September 12, 2024, PRIV provided the OIG with the decision memorandum[6] which officially approved the adoption of the model.[7] On September 13, 2024, the OIG reviewed the documentation provided and confirmed that it met the intent of the recommendation.

We request that OIG consider this recommendation resolved and closed, as implemented.

Recommendation 9: Develop and implement a formalized process for tracking and closing Privacy Compliance Review recommendations.

Response: Concur. PRIV currently tracks open PCR recommendations using “quad charts,”[8] and is developing a standard operating procedure for PCR follow-up that—once complete—will formalize PRIV’s process for tracking and closing recommendations. Further, as previously mentioned, PRIV will also formalize tracking through PRIVCATS in a future system update. ECD: November 28, 2025.

OIG recommended that the DHS Office for Civil Rights and Civil Liberties (CRCL):

Recommendation 10: Evaluate the personnel resources needed to meet civil rights and civil liberties oversight requirements and act as needed based on the results of the evaluation.

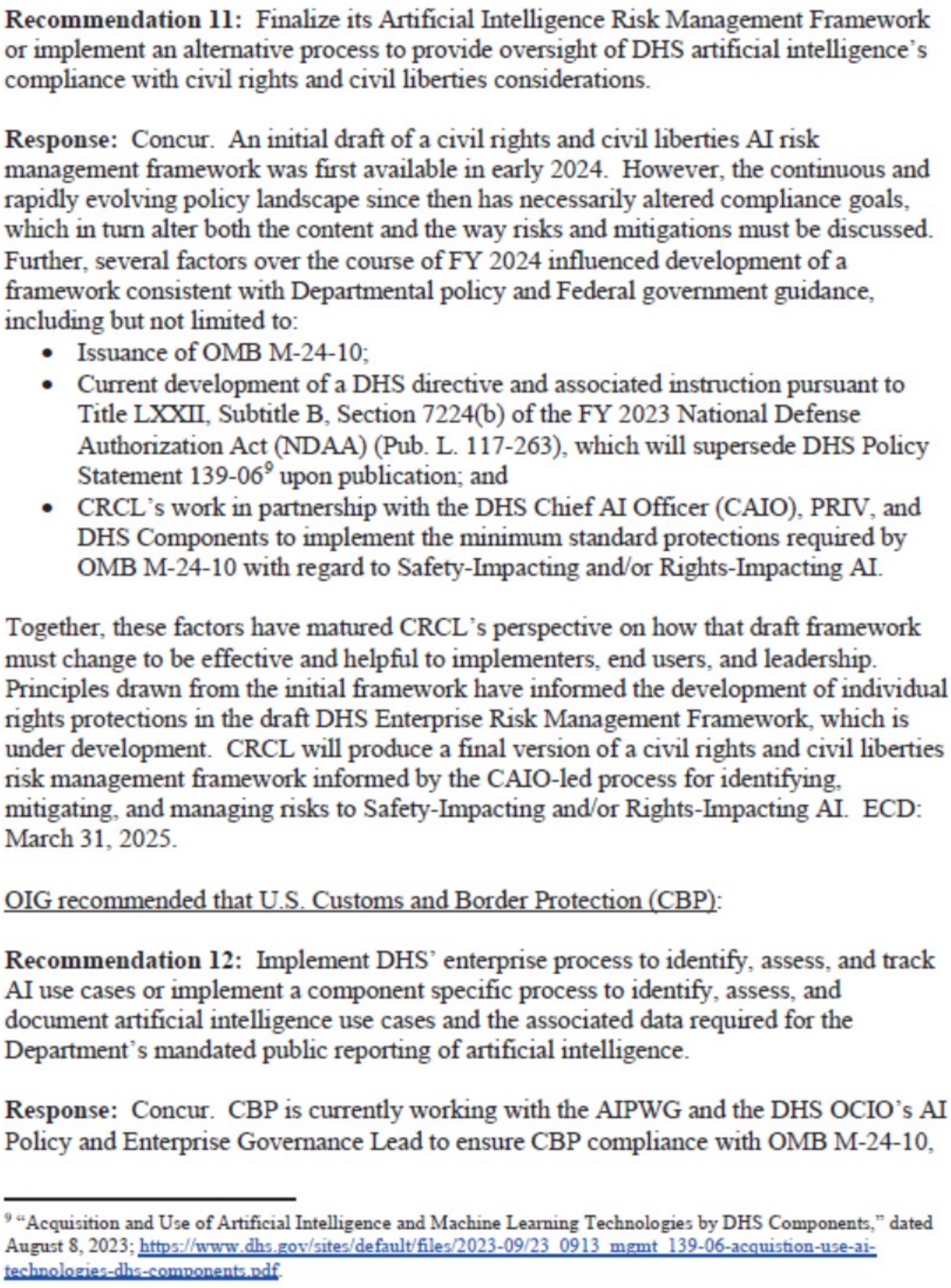
Response: Concur. CRCL evaluated resource needs to provide policy advice, conduct oversight activities, and support training requirements associated with Department’s adoption of AI. Specifically, from March 2024 to June 2024, CRCL participated in the DHS FY 2026-2030 AI Issue Team led by the DHS Office of the OCFO PA&E. As part of this evaluation, the AI Issue Team assessed DHS’s AI priorities, identified the Department’s capability gaps, and presented funding options that close or reduce the identified gaps. CRCL’s participation resulted in a baseline capability assessment of current CRCL resources, a gap analysis, and funding options, which was taken into consideration into the Department’s FY 2026 budget request so that CRCL could effectively support the Department’s AI activities. CRCL provided the OIG with documentation of these efforts on December 4, 2024.

We request that OIG consider this recommendation resolved and closed, as implemented.

[6] “DHS Privacy Office Privacy Compliance Review Prioritization 20240906 FINAL,” dated September 6, 2024.

[7] “Privacy Compliance Review Prioritization Model,” dated September 6, 2024.

[8] A quad chart is a visual summary of a project or program that's divided into four quadrants on a single page or slide. The Privacy Office’s Oversight Team maintains the quad charts. PRIV’s quad charts for PCRs with open recommendations include summary information at a point in time with the PCR description, PCR recommendation status information, major milestone status, risks or issues that may impact recommendation implementation, recent accomplishments, and next steps.



Recommendation 11: Finalize its Artificial Intelligence Risk Management Framework or implement an alternative process to provide oversight of DHS artificial intelligence's compliance with civil rights and civil liberties considerations.

Response: Concur. An initial draft of a civil rights and civil liberties AI risk management framework was first available in early 2024. However, the continuous and rapidly evolving policy landscape since then has necessarily altered compliance goals, which in turn alter both the content and the way risks and mitigations must be discussed. Further, several factors over the course of FY 2024 influenced development of a framework consistent with Departmental policy and Federal government guidance, including but not limited to:

- Issuance of OMB M-24-10;
- Current development of a DHS directive and associated instruction pursuant to Title LXXII, Subtitle B, Section 7224(b) of the FY 2023 National Defense Authorization Act (NDAA) (Pub. L. 117-263), which will supersede DHS Policy Statement 139-06[9] upon publication; and
- CRCL's work in partnership with the DHS Chief AI Officer (CAIO), PRIV, and DHS Components to implement the minimum standard protections required by OMB M-24-10 with regard to Safety-Impacting and/or Rights-Impacting AI.

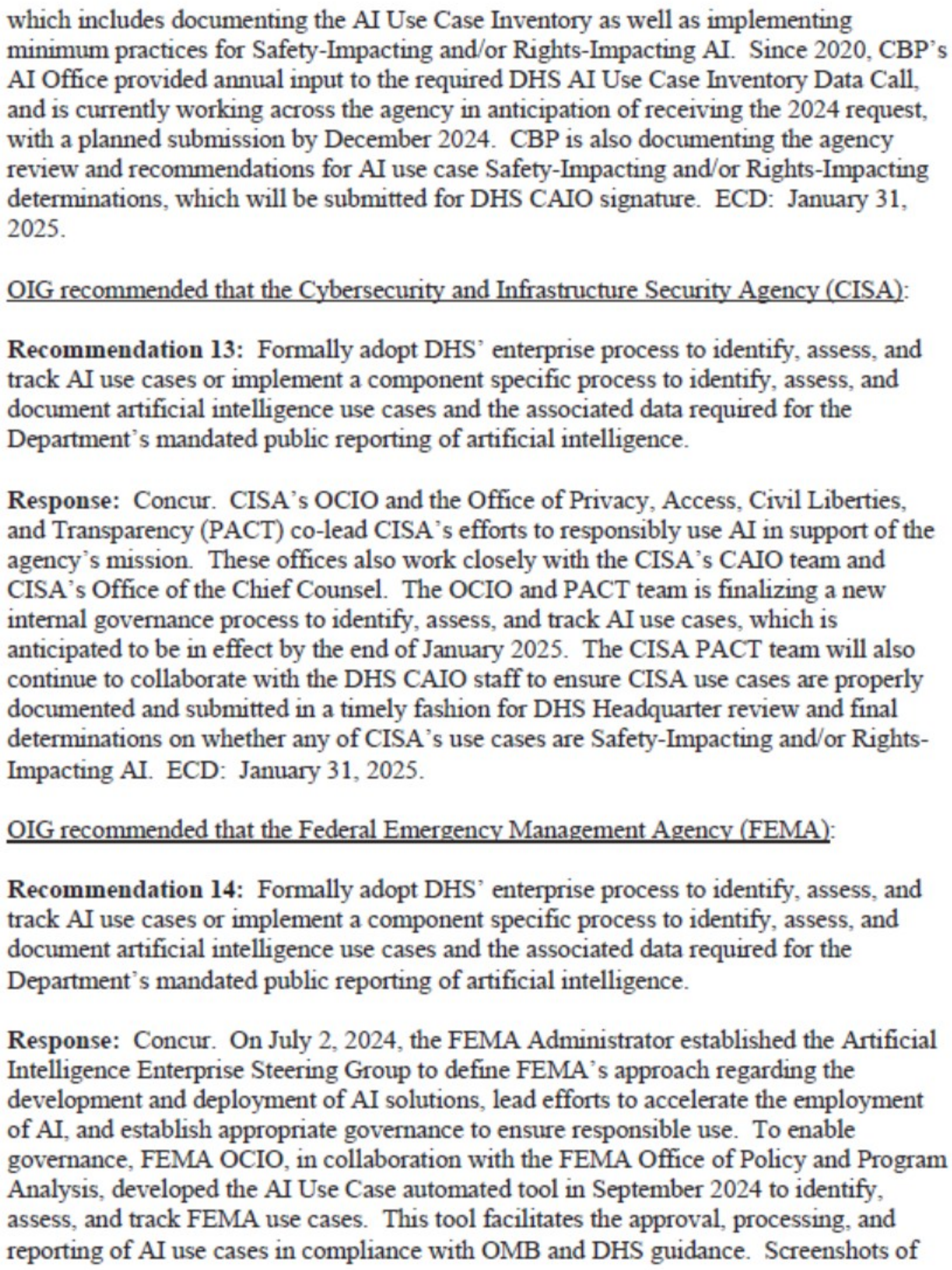
Together, these factors have matured CRCL's perspective on how that draft framework must change to be effective and helpful to implementers, end users, and leadership. Principles drawn from the initial framework have informed the development of individual rights protections in the draft DHS Enterprise Risk Management Framework, which is under development. CRCL will produce a final version of a civil rights and civil liberties risk management framework informed by the CAIO-led process for identifying, mitigating, and managing risks to Safety-Impacting and/or Rights-Impacting AI. ECD: March 31, 2025.

OIG recommended that U.S. Customs and Border Protection (CBP):

Recommendation 12: Implement DHS' enterprise process to identify, assess, and track AI use cases or implement a component specific process to identify, assess, and document artificial intelligence use cases and the associated data required for the Department's mandated public reporting of artificial intelligence.

Response: Concur. CBP is currently working with the AIPWG and the DHS OCIO's AI Policy and Enterprise Governance Lead to ensure CBP compliance with OMB M-24-10,

[9] "Acquisition and Use of Artificial Intelligence and Machine Learning Technologies by DHS Components," dated August 8, 2023; https://www.dhs.gov/sites/default/files/2023-09/23_0913_mgmt_139-06-acquistion-use-ai-technologies-dhs-components.pdf.



which includes documenting the AI Use Case Inventory as well as implementing minimum practices for Safety-Impacting and/or Rights-Impacting AI. Since 2020, CBP's AI Office provided annual input to the required DHS AI Use Case Inventory Data Call, and is currently working across the agency in anticipation of receiving the 2024 request, with a planned submission by December 2024. CBP is also documenting the agency review and recommendations for AI use case Safety-Impacting and/or Rights-Impacting determinations, which will be submitted for DHS CAIO signature. ECD: January 31, 2025.

OIG recommended that the Cybersecurity and Infrastructure Security Agency (CISA):

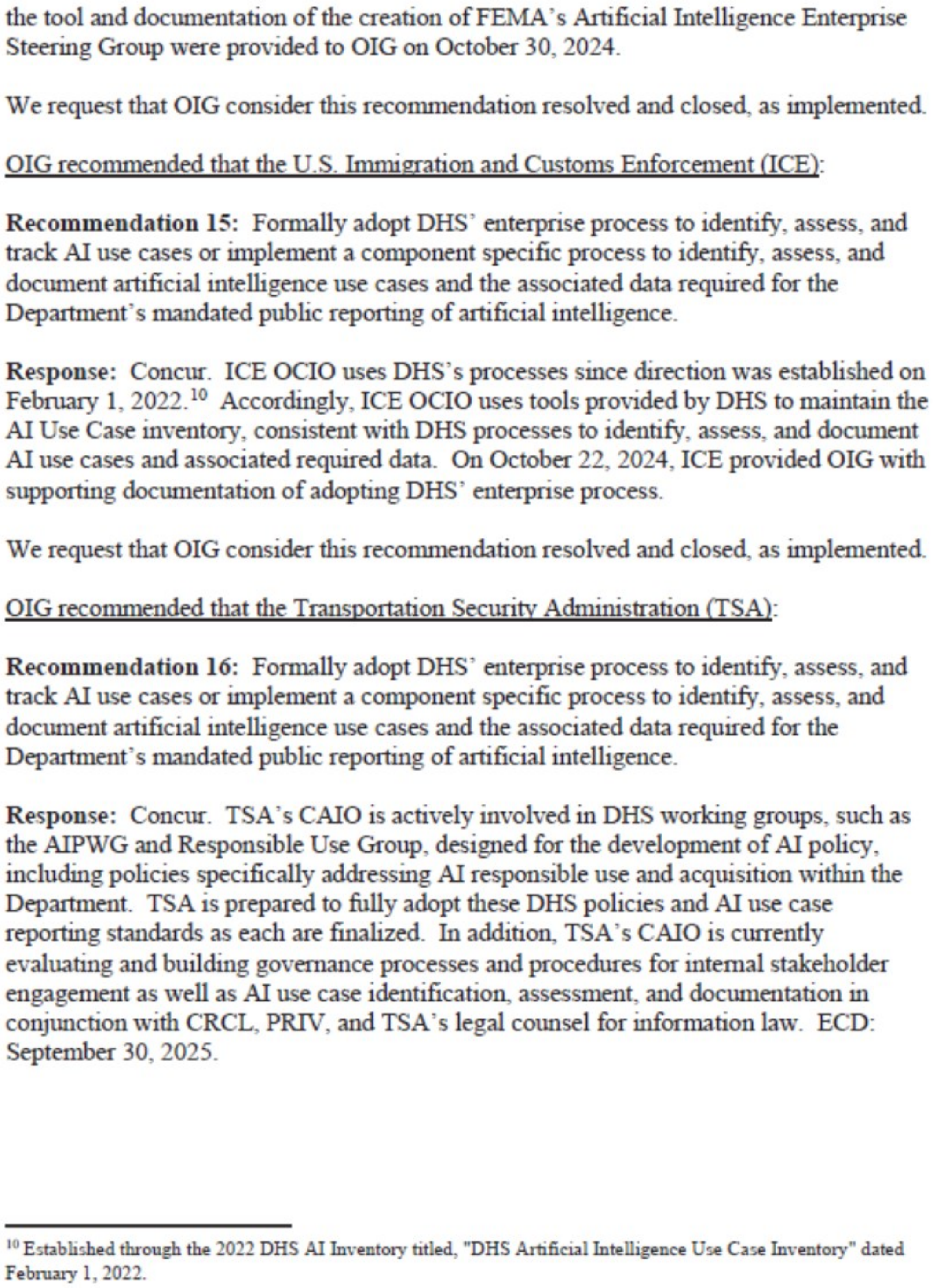
Recommendation 13: Formally adopt DHS' enterprise process to identify, assess, and track AI use cases or implement a component specific process to identify, assess, and document artificial intelligence use cases and the associated data required for the Department's mandated public reporting of artificial intelligence.

Response: Concur. CISA's OCIO and the Office of Privacy, Access, Civil Liberties, and Transparency (PACT) co-lead CISA's efforts to responsibly use AI in support of the agency's mission. These offices also work closely with the CISA's CAIO team and CISA's Office of the Chief Counsel. The OCIO and PACT team is finalizing a new internal governance process to identify, assess, and track AI use cases, which is anticipated to be in effect by the end of January 2025. The CISA PACT team will also continue to collaborate with the DHS CAIO staff to ensure CISA use cases are properly documented and submitted in a timely fashion for DHS Headquarter review and final determinations on whether any of CISA's use cases are Safety-Impacting and/or Rights-Impacting AI. ECD: January 31, 2025.

OIG recommended that the Federal Emergency Management Agency (FEMA):

Recommendation 14: Formally adopt DHS' enterprise process to identify, assess, and track AI use cases or implement a component specific process to identify, assess, and document artificial intelligence use cases and the associated data required for the Department's mandated public reporting of artificial intelligence.

Response: Concur. On July 2, 2024, the FEMA Administrator established the Artificial Intelligence Enterprise Steering Group to define FEMA's approach regarding the development and deployment of AI solutions, lead efforts to accelerate the employment of AI, and establish appropriate governance to ensure responsible use. To enable governance, FEMA OCIO, in collaboration with the FEMA Office of Policy and Program Analysis, developed the AI Use Case automated tool in September 2024 to identify, assess, and track FEMA use cases. This tool facilitates the approval, processing, and reporting of AI use cases in compliance with OMB and DHS guidance. Screenshots of



the tool and documentation of the creation of FEMA's Artificial Intelligence Enterprise Steering Group were provided to OIG on October 30, 2024.

We request that OIG consider this recommendation resolved and closed, as implemented.

OIG recommended that the U.S. Immigration and Customs Enforcement (ICE):

Recommendation 15: Formally adopt DHS' enterprise process to identify, assess, and track AI use cases or implement a component specific process to identify, assess, and document artificial intelligence use cases and the associated data required for the Department's mandated public reporting of artificial intelligence.

Response: Concur. ICE OCIO uses DHS's processes since direction was established on February 1, 2022.[10] Accordingly, ICE OCIO uses tools provided by DHS to maintain the AI Use Case inventory, consistent with DHS processes to identify, assess, and document AI use cases and associated required data. On October 22, 2024, ICE provided OIG with supporting documentation of adopting DHS' enterprise process.

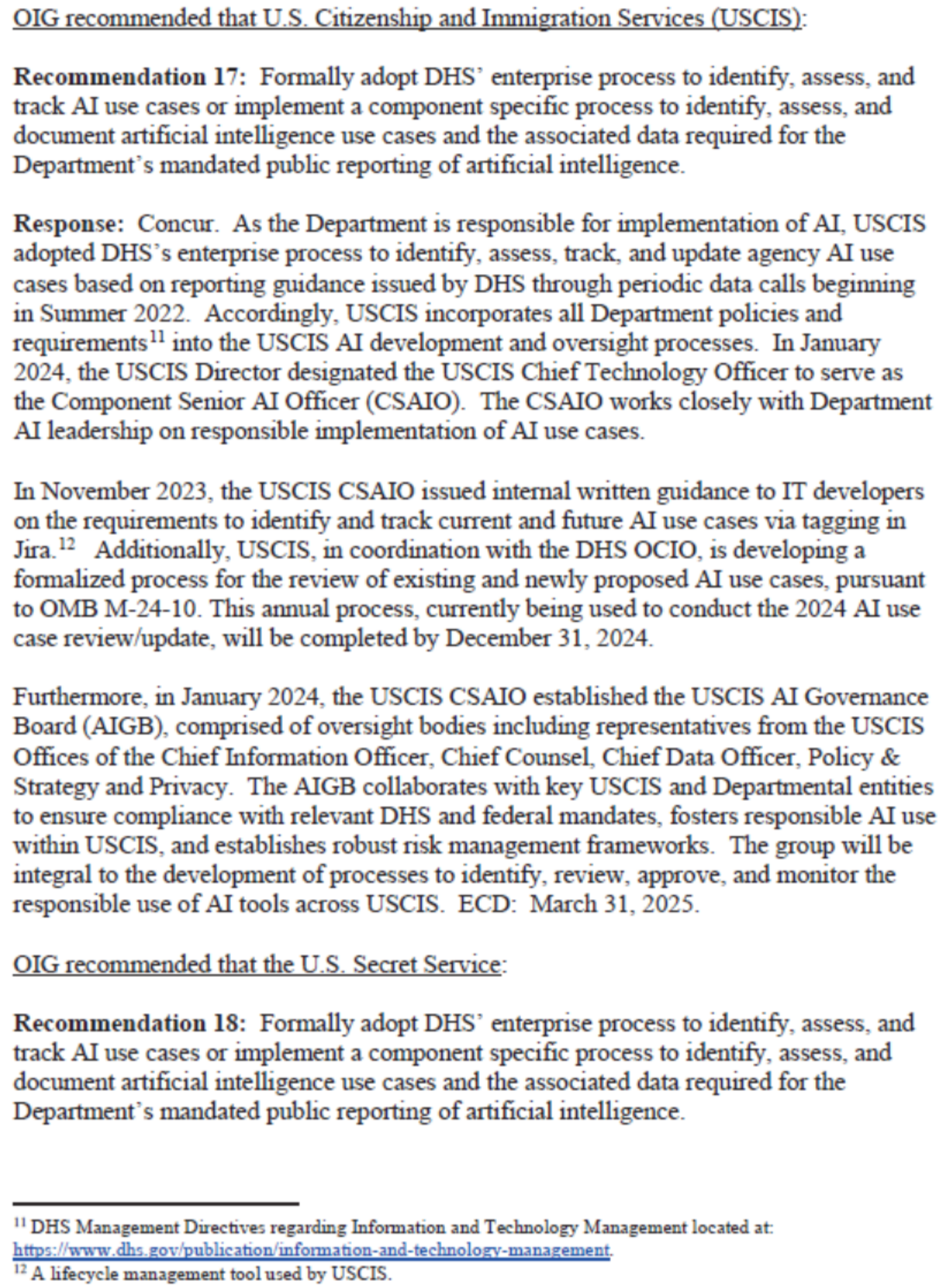
We request that OIG consider this recommendation resolved and closed, as implemented.

OIG recommended that the Transportation Security Administration (TSA):

Recommendation 16: Formally adopt DHS' enterprise process to identify, assess, and track AI use cases or implement a component specific process to identify, assess, and document artificial intelligence use cases and the associated data required for the Department's mandated public reporting of artificial intelligence.

Response: Concur. TSA's CAIO is actively involved in DHS working groups, such as the AIPWG and Responsible Use Group, designed for the development of AI policy, including policies specifically addressing AI responsible use and acquisition within the Department. TSA is prepared to fully adopt these DHS policies and AI use case reporting standards as each are finalized. In addition, TSA's CAIO is currently evaluating and building governance processes and procedures for internal stakeholder engagement as well as AI use case identification, assessment, and documentation in conjunction with CRCL, PRIV, and TSA's legal counsel for information law. ECD: September 30, 2025.

[10] Established through the 2022 DHS AI Inventory titled, "DHS Artificial Intelligence Use Case Inventory" dated February 1, 2022.



OIG recommended that U.S. Citizenship and Immigration Services (USCIS):

Recommendation 17: Formally adopt DHS' enterprise process to identify, assess, and track AI use cases or implement a component specific process to identify, assess, and document artificial intelligence use cases and the associated data required for the Department's mandated public reporting of artificial intelligence.

Response: Concur. As the Department is responsible for implementation of AI, USCIS adopted DHS's enterprise process to identify, assess, track, and update agency AI use cases based on reporting guidance issued by DHS through periodic data calls beginning in Summer 2022. Accordingly, USCIS incorporates all Department policies and requirements[11] into the USCIS AI development and oversight processes. In January 2024, the USCIS Director designated the USCIS Chief Technology Officer to serve as the Component Senior AI Officer (CSAIO). The CSAIO works closely with Department AI leadership on responsible implementation of AI use cases.

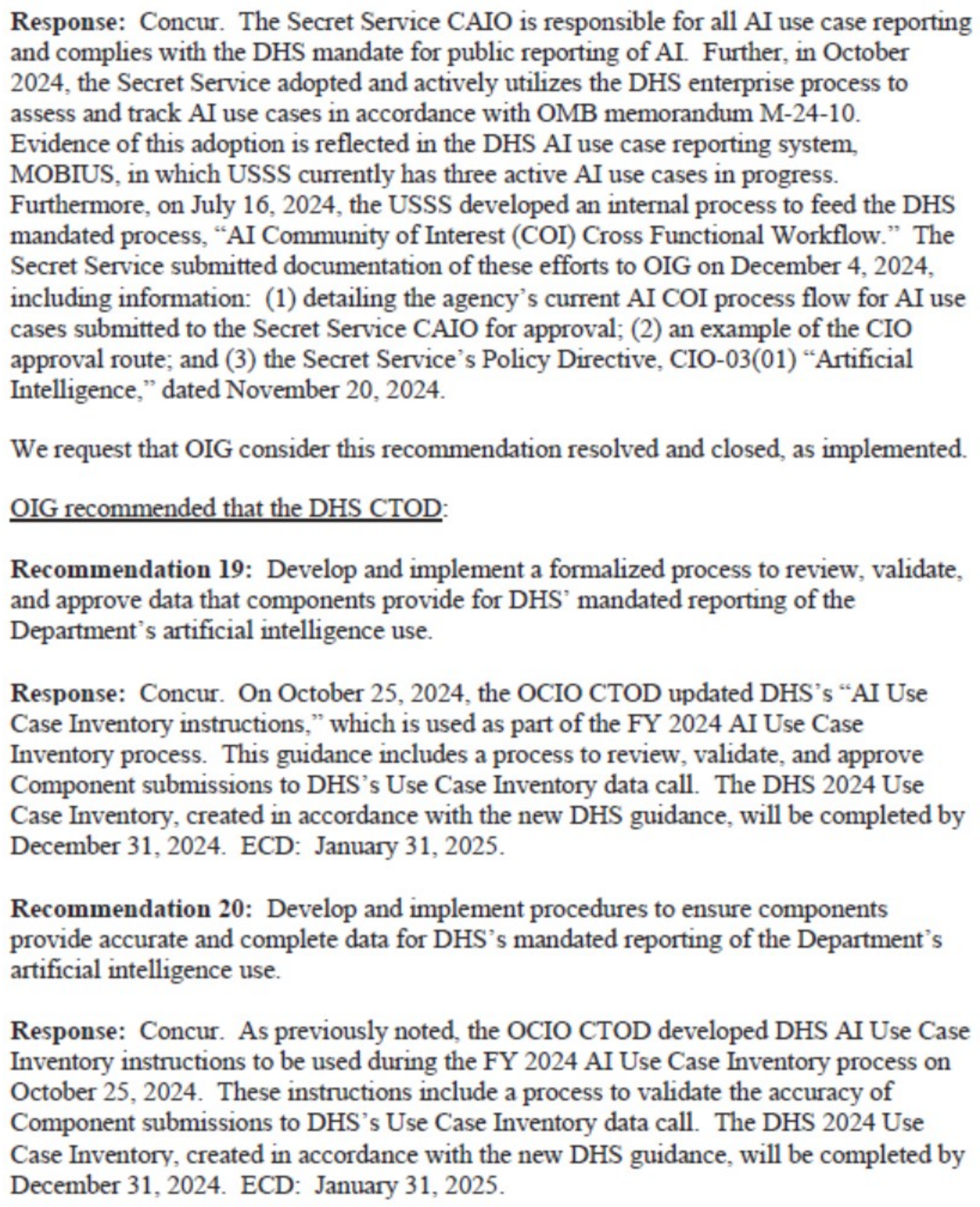
In November 2023, the USCIS CSAIO issued internal written guidance to IT developers on the requirements to identify and track current and future AI use cases via tagging in Jira.[12] Additionally, USCIS, in coordination with the DHS OCIO, is developing a formalized process for the review of existing and newly proposed AI use cases, pursuant to OMB M-24-10. This annual process, currently being used to conduct the 2024 AI use case review/update, will be completed by December 31, 2024.

Furthermore, in January 2024, the USCIS CSAIO established the USCIS AI Governance Board (AIGB), comprised of oversight bodies including representatives from the USCIS Offices of the Chief Information Officer, Chief Counsel, Chief Data Officer, Policy & Strategy and Privacy. The AIGB collaborates with key USCIS and Departmental entities to ensure compliance with relevant DHS and federal mandates, fosters responsible AI use within USCIS, and establishes robust risk management frameworks. The group will be integral to the development of processes to identify, review, approve, and monitor the responsible use of AI tools across USCIS. ECD: March 31, 2025.

OIG recommended that the U.S. Secret Service:

Recommendation 18: Formally adopt DHS' enterprise process to identify, assess, and track AI use cases or implement a component specific process to identify, assess, and document artificial intelligence use cases and the associated data required for the Department's mandated public reporting of artificial intelligence.

[11] DHS Management Directives regarding Information and Technology Management located at: https://www.dhs.gov/publication/information-and-technology-management.
[12] A lifecycle management tool used by USCIS.



Response: Concur. The Secret Service CAIO is responsible for all AI use case reporting and complies with the DHS mandate for public reporting of AI. Further, in October 2024, the Secret Service adopted and actively utilizes the DHS enterprise process to assess and track AI use cases in accordance with OMB memorandum M-24-10. Evidence of this adoption is reflected in the DHS AI use case reporting system, MOBIUS, in which USSS currently has three active AI use cases in progress. Furthermore, on July 16, 2024, the USSS developed an internal process to feed the DHS mandated process, "AI Community of Interest (COI) Cross Functional Workflow." The Secret Service submitted documentation of these efforts to OIG on December 4, 2024, including information: (1) detailing the agency's current AI COI process flow for AI use cases submitted to the Secret Service CAIO for approval; (2) an example of the CIO approval route; and (3) the Secret Service's Policy Directive, CIO-03(01) "Artificial Intelligence," dated November 20, 2024.

We request that OIG consider this recommendation resolved and closed, as implemented.

OIG recommended that the DHS CTOD:

Recommendation 19: Develop and implement a formalized process to review, validate, and approve data that components provide for DHS' mandated reporting of the Department's artificial intelligence use.

Response: Concur. On October 25, 2024, the OCIO CTOD updated DHS's "AI Use Case Inventory instructions," which is used as part of the FY 2024 AI Use Case Inventory process. This guidance includes a process to review, validate, and approve Component submissions to DHS's Use Case Inventory data call. The DHS 2024 Use Case Inventory, created in accordance with the new DHS guidance, will be completed by December 31, 2024. ECD: January 31, 2025.

Recommendation 20: Develop and implement procedures to ensure components provide accurate and complete data for DHS's mandated reporting of the Department's artificial intelligence use.

Response: Concur. As previously noted, the OCIO CTOD developed DHS AI Use Case Inventory instructions to be used during the FY 2024 AI Use Case Inventory process on October 25, 2024. These instructions include a process to validate the accuracy of Component submissions to DHS's Use Case Inventory data call. The DHS 2024 Use Case Inventory, created in accordance with the new DHS guidance, will be completed by December 31, 2024. ECD: January 31, 2025.

Appendix C:
Office of Audits Major Contributors to This Report

Tarsha Cary, Director
Alexander Stewart, Audit Manager
Alexandria Castaneda, Auditor-in-Charge
Tessa Clement, Auditor
Jessica Ionescu, Auditor
Dario Gutierrez, Auditor
Christine Viray, Auditor
Xavier Hill, Auditor
Maria Romstedt, Communications Analyst
Romina Ballmer, Independent Referencer

Appendix D:
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Under Secretary, Office of Strategy, Policy, and Plans
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Audit Liaison, CBP
Audit Liaison, CISA
Audit Liaison, FEMA
Audit Liaison, ICE
Audit Liaison, TSA
Audit Liaison, USCIS
Audit Liaison, USSS

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Additional Information

To view this and any other DHS OIG reports, Please visit our website: www.oig.dhs.gov

For further information or questions, please contact the DHS OIG Office of Public Affairs via email: DHS-OIG.OfficePublicAffairs@oig.dhs.gov

DHS OIG Hotline

To report fraud, waste, abuse, or criminal misconduct involving U.S. Department of Homeland Security programs, personnel, and funds, please visit: www.oig.dhs.gov/hotline

If you cannot access our website, please contact the hotline by phone or mail:

Call: 1-800-323-8603

U.S. Mail:
Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive SW
Washington, DC 20528-0305