Advancing Governance, Innovation, and Risk Management for the Use of Artificial Intelligence (AI) at the Department of Homeland Security (DHS)

DHS: Compliance Plan for Office of Management and Budget (OMB) Memoranda M-24-10 – September 2024

Prepared by Chief AI Officer Eric Hysen

Table of Contents

1 Strengthening AI Governance

1.1 General

DHS is committed to the safe, secure, responsible, and trustworthy use of AI in securing the homeland. This commitment includes establishing clear and effective governance and oversight for the use and acquisition of AI; protection for privacy, civil rights, and civil liberties; rigorous testing and evaluation to minimize inappropriate bias and disparate impact; and ongoing monitoring of the technology during operations to ensure continued compliance and delivery of intended outcomes. We believe the use of AI must be transparent, accountable, and explainable to the people the Department serves and the operators using this technology.

DHS continues to increase the breadth, depth, and maturity of AI's application across the Department. As early as 2015, the Department piloted the use of machine learning (ML) technologies to support identity verification tasks. Since then, DHS has successfully implemented other AI-powered applications to enhance efficiencies and foster innovation in border security, cybersecurity, immigration, trade, transportation safety, workforce productivity, and other domains critical to protecting the homeland.

As demonstrated through the activities outlined in this document, DHS understands that the Department must continue to ensure AI is used responsibly to advance the homeland security mission while protecting the privacy, civil rights, and civil liberties of the American public. With a talented and dedicated team of 260,000 personnel in 22 agencies and offices across the country and around the world, Americans interact daily with DHS more than with any other federal entity.

DHS has undertaken a coordinated, ongoing approach to ensuring safe, secure, responsible, and trustworthy use of AI. Our efforts include establishing guiding principles for AI use at DHS, piloting innovative uses of AI, and enhancing governance and oversight of AI use at DHS. Following the release of OMB M-24-10, *Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence*, on March 28, 2024, the Department began implementing the requirements.

Additionally, as part of Department's coordinated, ongoing approach to ensuring safe, secure, responsible, and trustworthy use of AI, DHS has been developing an enterprise policy to provide an overarching framework for advancing AI innovation and AI governance while managing risks from the use of AI, particularly those affecting the safety or rights of the public. This will build on our existing guiding principles for AI use and include considerations for privacy, civil rights, and civil liberties impacts; and security against misuse, degradation, or rendering inoperable of AI-enabled systems. This policy will also incorporate and address requirements in M-24-10 to advance governance, innovation, and risk management of AI at DHS.

1.2 DHS AI Governance Board

DHS has continued to strengthen our AI governance posture by designating a Chief Artificial Intelligence Officer (CAIO) and convening our AI Governance Board. DHS named Eric Hysen, our DHS Chief Information Officer, as the CAIO in September 2023 and officially designated him in April 2024, which satisfies the requirements under OMB M-24-10, Section (a)(i). The Department convened

our DHS AI Governance Board on May 17, 2024, fulfilling the requirements under OMB M-24-10, Section (a)(ii), and EO 144110, Section 10.b(1).

In establishing the DHS AI Governance Board, the Department leveraged an existing DHS leadership group, the Deputy's Management Action Group (DMAG). The DMAG will meet as the DHS AI Governance Board semi-annually, or more frequently as needed. The Board coordinates and governs issues related to the use of AI within DHS, including removing barriers to the use of AI and managing its associated risks. The Deputy Secretary of Homeland Security (Deputy Secretary) is the Chair of the Board and the DHS CAIO serves as the Vice Chair. The DHS CAIO supports the Deputy Secretary, through the Board, in coordinating AI activities across the Department and implementing the Department's responsibilities under EO 14110.

DHS AI Governance Board membership includes appropriate representation from senior officials responsible for key enablers of AI adoption and risk management, including at least information technology, cybersecurity, data, privacy, civil rights and civil liberties, equity, statistics, human capital, procurement, budget, legal, agency management, customer experience, program evaluation, and officials responsible for implementing AI with an agency's program office(s).

The DHS AI Governance Board is comprised of the following senior DHS officials:

- **Deputy Secretary of Homeland Security, as the Chair**
- **DHS Chief Artificial Intelligence Officer, as the Vice-Chair**
- DHS Chief of Staff
- Under Secretary for Management
- Under Secretary, Office of Strategy, Policy, and Plans
- Under Secretary, Office of Science and Technology
- Under Secretary, Office of Intelligence and Analysis
- Under Secretary, Countering Weapons of Mass Destruction
- DHS Chief Financial Officer
- DHS Chief Information Officer
- DHS Chief Privacy Officer
- DHS Officer for Civil Rights and Civil Liberties
- General Counsel
- Deputy Director, Cybersecurity and Infrastructure Security Agency
- Deputy Commissioner, Customs and Border Patrol
- Deputy Administrator, Federal Emergency Management Agency
- Deputy Director, Federal Law Enforcement Training Centers
- Deputy Director, Immigration and Customs Enforcement
- Deputy Director, Office of Homeland Security Situational Awareness Deputy Administrator, Transportation Security Administration
- Deputy Director, US Citizenship and Immigration Services
- Deputy Commandant, US Coast Guard
- Deputy Director, US Secret Service

The Board serves as the primary coordination entity among DHS officials responsible for aspects of AI adoption and risk management. Accordingly, the Board will provide oversight and leadership for ensuring safety- and/or rights-impacting AI use cases across DHS comply with minimum practices outlined in Section 5 of OMB M-24-10, or else are retired. A key piece of the Board's impact has been

organizational clarity and responsibility regarding adequate testing and evaluation. The Board will also provide strategic direction for the Department's ongoing engagement with external stakeholders on a variety of AI-related topics.

In fulfilling the commitments in the DHS AI Roadmap, discussed further below in Section 2.1, the Department has been expanding strategic partnerships within and outside established channels, including with the private sector, academia, State, Local, and Tribal governments, international partners, non-government organizations, thought leaders, and communities, advocates, and partners. The Board's strategic direction involves responsive actions to the feedback and information from this ongoing engagement. Related to engagement and public feedback, the Board has prioritized the Department's AI Use Case Inventory as a primary vehicle for providing transparency and fostering trust in DHS's use of AI. The Board has already directed that, in updating the Inventory in 2024 in accordance with OMB's annual guidance, the Department must ensure consistency across the Department in how, when, and to what extent, AI use cases are reported in the Inventory.

1.3 DHS AI Use Case Inventory

Since 2022, DHS has been publishing a public inventory of DHS AI use cases in accordance with requirements in EO 13960 *Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government* (December 2020), and the Advancing American AI Act (December 2022). The DHS AI Use Case Inventory contains information on AI use cases that can be publicly disclosed consistent with applicable law or government-wide policy. The Department acknowledges that in the past our public-facing AI use case inventory descriptions have sometimes been incomplete or limited, and that this can lead to misunderstandings. We are working to provide greater clarity in our AI use case inventory going forward. DHS updates this inventory annually in accordance with OMB's annual guidance regarding Federal agencies' use case inventories and provides other updates, on an ongoing basis, as necessary to keep the inventory accurate.

For annual updates in accordance with OMB guidance, as well as other ongoing updates to the DHS AI Use Case Inventory, DHS solicits and collates information about existing use cases and any new use cases from across-the Department. Senior officials responsible for AI within a Component and across the Department, DHS personnel responsible for AI use cases within each Component, legal counsel, and subject matter experts familiar with specific DHS AI use cases all support and participate in the solicitation and collation of information about AI use cases. The information solicited aligns with the information required in OMB's annual guidance for each use case already listed on the DHS AI Use Case Inventory, as well as information about any new AI use cases since the last solicitation. The process for this generally includes:

- Initiating a solicitation and collation request from the DHS Office of the Chief Information Officer (OCIO) / Chief AI Officer (OCAIO)
- Responses to the request from DHS Components
- Review of the responses with the OCIO/OCAIO and any follow-up necessary
- Collation of the information for review and approval by the DHS CAIO

Of note, the solicitation and collation for the 2024 annual update will include information regarding whether each DHS AI use case reported in the DHS AI Use Case Inventory is safety- and/or rights-impacting, and information about compliance with the minimum practices outlined in Section 5 of OMB M-24-10. The DHS 2024 updates will fully comply with the OMB guidance for 2024 AI Reporting per

EO 14110. The 2024 annual update also will address the AI Governance Board's direction to ensure consistency across the Department in how, when, and to what extent, AI use cases are reported in the Inventory. DHS will publish the version of the DHS AI Use Case Inventory incorporating the 2024 annual updates in alignment with the December 16, 2024, deadline provided by OMB.

1.4 Reporting on AI Use Cases Not Subject to Inventory

DHS is implementing the new aggregate reporting requirement in Section 3(a)(v) of OMB M-24-10 as part of the process for soliciting and collating information for the 2024 annual update to the DHS AI Use Case Inventory. Section 3(a)(v) requires that AI use cases not required to be individually inventoried must be reported through aggregate metrics about the use cases, including number of such use cases that are safety- and/or rights-impacting and their compliance with the minimum practices outlined in Section 5 of OMB M-24-10.

DHS has some AI use cases that are not included in the DHS AI Use Case Inventory because public disclosure of the use case would be inconsistent with applicable law or government-wide policy. For oversight and governance purposes, DHS already tracks such use cases. DHS plans to re-review these use cases to determine whether any information about the use case could be publicly released and partially reported on the DHS AI Use Case Inventory. This re-review includes consultation with legal counsel regarding applicable law and policy governing public disclosure. For AI use cases that cannot be publicly released and partially reported on the DHS AI Use Case Inventory, DHS will report aggregate metrics in accordance with Section 3(a)(v) of OMB M-24-10.

As part of the process for soliciting and collating information for the 2024 annual updates to the DHS AI Use Case Inventory (outlined in section 1.3 of this document), DHS will re-review AI use cases that previously have not been publicly disclosed and collect the information necessary to either partially report on the DHS AI Use Case Inventory or fulfill the aggregate reporting requirements. To do this, the solicitation and collation request from with the Office of the DHS Chief Information Officer / DHS Chief AI Officer will include: (1) re-review with legal counsel those AI use cases that previously have not been publicly disclosed, and (2) determination with legal counsel whether those use cases can be fully or partially reported on the DHS AI Use Case Inventory, and if not, information necessary to include those use cases in aggregate reporting.

Starting in 2025, DHS plans to annually re-review AI use cases that are not included in the DHS AI Use Case Inventory because public disclosure of the use case would be inconsistent with applicable law or government-wide policy. DHS plans to incorporate this re-review into its process for annual updates to the DHS AI Use Case Inventory.

2 Advancing Responsible AI Innovation

2.1 AI Strategy

DHS maintains a clear set of principles and robust governance that prioritizes the protection of privacy, civil rights, and civil liberties. The Department's approach is the foundation for its work to ensure Artificial Intelligence (AI) is used responsibly across its unique missions. Secretary Alejandro N. Mayorkas established guiding principles for the responsible use of AI in Policy Statement 139-06: Acquisition and Use of AI and ML by DHS Components. The policy statement establishes the

foundation for DHS's use of AI with a clear set of principles. These principles include that DHS systems, programs, and activities using AI will conform to the requirements of Executive Order 13960, Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government. In addition, DHS will only acquire and use AI in a manner that is consistent with the Constitution and all other applicable laws and policies. Also, DHS will not collect, use, or disseminate data used in AI activities, or establish AI-enabled systems that make or support decisions, based on the inappropriate consideration of race, ethnicity, gender, national origin, religion, gender, sexual orientation, gender identity, age, nationality, medical condition, or disability.

In April 2024, DHS published its first AI Roadmap which details plans to test uses of the technologies that deliver meaningful benefits to the American public and advance homeland security, while ensuring that individuals' privacy, civil rights, and civil liberties are protected. The roadmap lays out DHS's initiatives in AI, describes the potential of AI technologies across the Department, and offers clearer visibility into the Department's approach to AI, while underscoring the Department's commitment to responsible utilization. The AI roadmap outlined the three lines of effort DHS is using to guide its work:

- Responsibly leverage AI to advance Homeland Security missions while protecting individuals' privacy, civil rights, and civil liberties
- Promote Nationwide AI Safety and Security
- Continue to lead in AI through strong cohesive partnerships

As part of the roadmap, DHS announced three innovative pilot projects that will deploy AI in specific mission areas. These pilot programs will allow the Department to assess the efficacy of AI in improving its mission capabilities. Each pilot team is partnering with privacy, cybersecurity, and civil rights and civil liberties experts throughout their development and evaluation process. This work will inform Department-wide policies on AI governance. DHS offices and agencies submitted dozens of proposals for consideration to the Chief AI Officer, who selected three pilots that would best support evaluating the effectiveness of Large Language Models (LLM) and Generative AI technology at DHS.

The Department intends to build on the AI Roadmap as it develops the AI Strategy required under Section 4(a) of OMB M-24-10. DHS will build on the AI Roadmap's initiatives, and lessons-learned from related activities, to create a strategy for identifying and removing barriers to the responsible use of AI and achieving enterprise-wide improvements in AI maturity.

2.2 Removing Barriers to the Responsible Use of AI

DHS has undertaken a coordinated, ongoing approach to addressing barriers to responsibly leveraging AI to advance the homeland security mission. This includes establishment of the AI Task Force, policy for the use of facial recognition and facial capture, and policy on the use of commercial generative AI.

- In April 2023, Secretary Mayorkas established the AI Task Force to address the many ways in which AI will alter the threat landscape. Ensuring the Department's use of AI is rigorously tested to avoid bias and disparate impact, and is clearly explainable to the people we serve, was a primary focus. The Task Force's initial focus was on combating fentanyl trafficking, strengthening supply chain security, countering child exploitation, and protecting critical infrastructure. As part of the Task Force, DHS created the Responsible Use Group, chaired by the DHS Officer for Civil Rights and Civil Liberties, to provide guidance, risk assessment,

mitigation strategies, and oversight for the protection of individual rights in projects championed by the Task Force. The Task Force has also provided leadership for established policy governing AI use and promoting innovation.

- In September 2023, DHS released our Directive (026-11) on the Use of Face Recognition and Face Capture Technologies. This directive dictates that all uses of face recognition and face capture technologies will be thoroughly tested to ensure there is no unintended bias or disparate impact in accordance with national standards. DHS will review all existing uses of this technology and conduct periodic testing and evaluation of all systems to meet performance goals. The Directive also requires that U.S. citizens be afforded the right to opt-out of face recognition for specific, non-law enforcement uses, prohibits face recognition from being used as the sole basis of any law or civil enforcement related action, and establishes a process for Department oversight offices including the Privacy Office, the Office for Civil Rights and Civil Liberties (CRCL), and the Office of the Chief Information Officer, to review all new uses of face recognition and face capture technologies.

- In October 2023, the Department released DHS Policy (139-07) on the Use of Commercial Generative AI (GenAI) Tools. This enabled and encouraged responsible use of commercial GenAI tools at DHS to ensure we continuously adapt to the future of work. Part of responsible use at DHS is considering how using these tools might impact privacy considerations. DHS considered these privacy impacts and appropriate mitigations in a privacy impact assessment (PIA). Additionally, the Department's policy establishes guidelines for the use of commercial GenAI tools by DHS personnel. The policy provides specific requirements and use limitations designed to safeguard data and protect privacy and individual rights. It also lays out a process for obtaining approval to use GenAI tools that includes the completion of training on the responsible use of AI and agreeing to follow rules of behavior when using these tools. The Department's public release of our GenAI resources, including our negotiated Terms of Service, has help other federal agencies fast-track their use of these tools

2.3 AI Talent

On February 6, 2024, Secretary Mayorkas and CIO/CAIO Eric Hysen announced the Department's first-ever hiring sprint to recruit 50 AI technology experts in 2024. Using the Office of Personnel Management's new flexible hiring authorities for AI-related jobs, including direct hire authorities, DHS worked to streamline and expedite the federal hiring to ensure qualified candidates received offers as quickly as possible. The new DHS "AI Corps" is modeled after the U.S. Digital Service and will support the Department to continue to leverage AI across the homeland security enterprise. The AI Corps is comprised of engineers, data scientists, project management professionals, and other technology experts.

As part of the Department's AI Corps hiring sprint, DHS has onboarded over 25 AI experts from the private and public sectors to play pivotal roles responsibly leveraging AI across strategic mission areas in the Department. The AI Corps is one of the most significant AI-talent recruitment efforts of any federal civilian agency, aiming to hire 50 AI experts to enhance service delivery and impact the homeland security mission while safeguarding privacy, civil rights, and civil liberties.

AI Corps members are currently working with the DHS Supply Chain Resilience Center to investigate how AI could be used to forecast the impacts of critical supply chain disruptions to public safety and security; working with DHS Science & Technology (S&T) to develop test and evaluation (T&E) requirements across the lifecycle of an AI system; and leveraging generative AI to support the work of the Department's Homeland Security Investigations (HSI) department to combat fentanyl, human trafficking, child exploitation, and other criminal networks.

As we look ahead to future AI hiring needs, we are adding AI competencies to the Cybersecurity Talent Management System (CTMS), a modernized personnel system that offers streamlined hiring, competitive compensation, and meaningful career development opportunities.

Additionally, in Fall 2023, DHS launched training on the use by DHS personnel of commercially available GenAI tools. This training provided the DHS workforce with information needed to use the DHS-approved tools responsibly. Thousands of employees and contractors from across the Department have completed this training. DHS OCIO is also holding recurring educational sessions to demonstrate how employees and contractors can apply GenAI at work. These sessions expand on the required training and are being used to highlight lessons learned and potential uses.

2.4 AI Sharing and Collaboration

DHS is moving toward a "default to open" approach to software development to promote transparency, sharing, and releasing of AI code in accordance with Section 4(d) of OMB M-24-10. Section 4(d) requires agencies to share their AI code, models, and data, and do so in a manner that facilitates re-use and collaboration government-wide and with the public, subject to applicable law, and guidance. Section 4 also requires considering: sharing and releasing AI custom-developed code, and AI data assets; partial sharing and release when some portion of AI code, models, or data cannot be shared or publicly released; procuring custom-developed code for AI, data to train and test AI, and enrichments to existing data in a manner that allows for the sharing and public release of relevant code, models, and data; and assessing the risk that AI models can be induced to reveal sensitive details of the data used to development them.

DHS introduced its "default to open" approach in September 2023 through Policy Directive 142-04 which also reinforced the DHS Source Code Inventory Process (SCIP). The DHS SCIP is a process for inventorying DHS custom-developed source code. The Policy Directive also requires specific guidance for how to release code as open source. The DHS CIO is responsible for implementing the DHS SCIP, in collaboration with the General Counsel, Office of the Chief Procurement Officers, the DHS Chief Privacy Officer, and DHS Component officials, including chief information officers, chief information security officers, and legal counsel.

The DHS SCIP comprises three main sub-processes: inventory, open source release, and inventory submission to Code.gov. The inventory process involves identifying and recording all DHS custom-developed code and comprises activities including determining usage types and defining metadata values for custom-developed code. The release process involves the transition of inventoried custom-developed code for public open source release to a publicly available repository and comprises activities including identifying appropriate open source licensing and performing security analyses of custom-developed code. The inventory submission process involves the verification and submission of the final custom-code inventory metadata to Code.gov, the government-wide source code inventory.

As outlined in Section 2.1, above, DHS is using our three GenAI pilots to assess the efficacy of AI in improving mission capabilities. These pilots will help us capture AI governance, innovation, and risk management best practices, informing future Department-wide policies. The lessons learned from these pilots will be beneficial in shaping how the Department leverages GenAI across DHS to further our mission to protect our homeland.

2.5 Harmonization of AI Requirements

DHS is committed to collaborative work harmonizing implementation of AI-related requirements within government and outside of government. DHS supports OMB's efforts to coordinate sharing resources and best practices in accordance with Section 4(e) of OMB M-24-10. Section 4(e) explains that OMB, in collaboration with the Office of Science and Technology Policy, will coordinate the development and use of AI in agencies' programs and operations across Federal agencies through an interagency council. The DHS CAIO serves on the OMB interagency council and DHS actively participates in the council's three working groups on GenAI, procurement, and risk management. In addition, DHS co-chairs the GenAI and procurement working groups.

DHS is also engaged in specific efforts to document and share best practices regarding AI governance, innovation, and risk management with Federal, State, and Local agency partners through collaborative meetings and the DHS AI webpages at dhs.gov/ai. The DHS AI webpages highlight the Department's innovative use of AI to secure the homeland and provides the Department's guiding principles and governing polices regarding the use of AI. Of note, DHS created a GenAI resources webpage in February 2023 as public repository for the resources it was already sharing with Federal, State, and Local partners: https://www.dhs.gov/publication/commercial-genai-resources.

For sharing AI-related best practices outside of government, DHS leverages the AI Safety and Security Board (AISSB). DHS established the AISSB in April 2024 pursuant to Section 4.3(a)(v) of E.O. 14110. The AISSB includes AI experts from the private sector and government that advise the Secretary and the critical infrastructure community. The AISSB provides information and recommendations for improving security, resilience, and incident response related to the use of AI.

3 Managing Risks from the Use of AI

3.1 Determining Which AI Is Presumed to Be Safety-Impacting or Rights-Impacting

In accordance with Section 5 of OMB M-24-10, DHS is reviewing its AI use cases to determine which use cases are safety- and/or rights-impacting and subject to the minimum practices outlined in Section 5. DHS is reviewing these use cases using a process similar to that outlined previously for soliciting and collating information about existing and new use cases from across DHS to update the DHS AI Use Case Inventory. The DHS Office of the Chief Information Officer (OCIO) / Chief AI Officer (OCAIO) issues a solicitation request asking for a recommendation or initial determinations for each AI use case across the Department regarding whether the use case is safety-impacting and/or rights-impacting. Such recommendations or initial determinations are made by senior officials responsible for AI within a Component and across the Department, DHS personnel responsible for AI use cases within each Component, legal counsel, and subject matter experts familiar with specific DHS AI use cases. The

CAIO reviews the recommendations or initial determinations in collaboration with the DHS Officer for Civil Rights and Civil Liberties and the DHS Chief Privacy Officer to make a final determination for each use case.

To determine whether a DHS AI use case is safety- and/or rights-impacting and subject to the minimum practices outlined in Section 5 of OMB M-24-10, each use case is evaluated using the following questions:

- Is the use case excluded from the scope of Section 5 and the minimum practices because it is (1) certain basic or applied research and development excluded in Section 2(b)(iv); (2) used within a national security system excluded in Section 2(c); or (3) within an element of the intelligence community excluded in Section 5?
- For use cases not excluded from the scope of Section 5:
    - Is the use case presumed safety-impacting based on the presumptive categories in M-24-10 Appendix I?
    - Regardless, does the use case meet the definition of "safety-impacting AI" in Section 6?
    - Is the use case presumed rights-impacting based on the presumptive categories in M-24-10 Appendix I?
    - Regardless, does the use case meet the definition of "rights-impacting" in Section 6?

For an AI use case that is presumed to be safety- and/or rights-impacting based on the presumptive categories in M-24-10 Appendix I, but that does not meet the definition of "safety-impacting AI" and/or "rights-impacting AI," the DHS CAIO may determine that the AI use case is not safety-impacting and/or rights-impacting. As provided in Section 5(b) of the OMB M-24-10, the DHS CAIO may make such a determination based on a documented context-specific and system-specific risk assessment. That assessment for DHS will be an analysis explaining why the use case does not meet the relevant definition(s). DHS anticipates that there may be some AI use cases at DHS that the DHS CAIO determines do not meet the definition of "safety-impacting AI" or "rights-impacting AI", but the DHS CAIO will still require to comply with the minimum risk management practices outlined in Section 5(c) of M-24-10.

DHS will publicly identify the DHS AI use cases that are determined to be safety- and/or rights impacting as part of the 2024 annual updates to the DHS AI Use Case Inventory discussed previously. In those updates, DHS will also identify the DHS AI uses cases that are presumed to be safety- and/or rights-impacting but that the DHS CAIO determined are not, in fact, safety- and/or rights-impacting in accordance with Section 5(b) requirements. For the DHS AI use cases determined to be safety- and/or rights-impacting that are not at least partially reported on the DHS AI Use Case Inventory because public disclosure of the use case would be inconsistent with applicable law or government-wide policy, DHS will publicly report aggregate metrics about these use cases as discussed previously. DHS will publish the 2024 annual updates to the DHS AI Use Case Inventory, and aggregate metrics, in alignment with the December 16, 2024 deadline provided by OMB annual updates to agencies' use case inventories.

3.2 Implementation of Risk Management Practices and Termination of Non-Compliant AI

DHS is implementing the minimum risk management practices outlined in Section 5(c) in accordance with the December 1, 2024 deadline. For DHS AI use cases that are determined to be safety- and/or

rights-impacting, as described previously, DHS is reviewing information about those use cases to ensure they satisfy the relevant pre-deployment practices outlined in Sections 5(c)(iv)(A)-(C) and 5(c)(v)(A)-(B) and the relevant post-deployment practices outlined in Sections 5(c)(iv)(D)-(I) and 5(c)(v)(C)-(F), as applicable, of the OMB M-24-10.

Use case information used for this review is information necessary to holistically assess the impact of the use case using the relevant, applicable pre-deployment and post-deployment practices. Such holistic assessment includes:

- identifying the intended purpose, expected benefits, and potential key risks of the use case;
- assessing the quality and appropriateness of the relevant data;
- determining whether the use case has been tested in operational or real-world environments, following domain-specific best practices, to understand the performance and impact it may have on affected individuals or communities;
- ensuring there is a process to monitor the use case's performance regarding functionality and any changes to its impact on safety or rights;
- identifying whether the use case carries out a decision or action without direct human involvement that could result in a significant impact on rights or safety and/or is used to significantly influence or inform decisions or actions that could have an adverse or negative impact on specific individuals or groups; and
- ensuring any required reasonable and timely notice of a use case is provided, as applicable.

Senior officials responsible for AI within a Component and across the Department, DHS personnel responsible for AI use cases within each Component, legal counsel, and subject matter experts familiar with specific DHS AI use cases are involved in providing use case information necessary to holistically assess the impact of the use case. Subject matter experts from the Offices of the Chief Information Office / Chief AI Officer, Office for Civil Rights and Civil Liberties and the Privacy Office, and the Science and Technology Directorate are involved in reviewing that information in advance of the DHS CAIO's independent evaluation of DHS AI use cases that are safety- and/or rights-impacting.

A key piece of ensuring consistent implementation across DHS is involving the DHS CAIO. The DHS CAIO will independently evaluate DHS AI use cases that are determined to be safety- and/or rights-impacting. The DHS CAIO will evaluate these use cases after the use case is reviewed to assess the impact of the use case using the relevant, applicable minimum risk management practices. The DHS CAIO will review information used for the holistic assessment, including information about testing and evaluation of the AI use case. As necessary and appropriate, the DHS CAIO will approve or disapprove continued use of AI use cases based on whether the use case satisfies the applicable pre-deployment and post-deployment practices.

For a DHS AI use case determined to be safety- and/or rights-impacting that does not satisfy one or more of the applicable minimum practices outlined in Section 5, the DHS CAIO may waive that required practice. As provided in Section 5(c)(iii) of OMB M-24-10, the DHS CAIO may waive one or more of the minimum practices with a written determination, based on upon a system-specific and context-specific risk assessment, that fulfilling the requirement would increase risks to safety or rights overall or would create an unacceptable impediment to critical agency operations. That determination will be made as part of the DHS CAIO's independent evaluation of the use case.

For a DHS AI use case determined to be safety- and/or rights-impacting that does not satisfy one or more of the applicable minimum practices, and for which the DHS CAIO does not provide a waiver

from that required practice, the DHS CAIO will terminate that AI use case, requiring that it be discontinued and retired. The process for discontinuing and retiring any such use case will be outlined with specific timelines as part of the DHS CAIO's independent evaluation of the use case and in consultation with the affected Component.

3.3 Minimum Risk Management Practices

DHS will publicly disclose its implementation of the minimum risk management practices outlined in Section 5(c) as part of the 2024 annual updates to the DHS AI Use Case Inventory discussed previously. In the DHS AI Use Case Inventory, DHS will publicly identify whether DHS AI use cases that are determined to be safety- and/or rights impacting comply with applicable minimum risk management practices, whether any such use case received a CAIO waiver of one or more of the applicable practices, and whether any such use case is being discontinued and retired because it does not comply with the applicable minimum practices. DHS will publish the 2024 annual updates to the DHS AI Use Case Inventory in alignment with the December 16, 2024, deadline provided by OMB annual updates to agencies' use case inventories.

Implementing the minimum risk management practices involves several key DHS officials and stakeholders. The DHS CAIO leads these efforts and ensures consistent implementation across DHS. The DHS Officer for Civil Rights and Civil Liberties and the DHS Chief Privacy Officer advise on final determinations regarding whether an AI use case is safety- and/or rights-impacting. These Officers, along with the Under Secretary for Science and Technology, also provide subject matter experts for reviewing use case information as part of assessing the impact of the use case to aid the DHS CAIO's independent evaluation of use cases that are safety- and/or rights-impacting. Additionally, Senior officials responsible for AI within a Component and across the Department, DHS personnel responsible for AI use cases within each Component, legal counsel, and subject matter experts familiar with specific DHS AI use cases are involved in providing use case information necessary to holistically assess the impact of the use case.