Department of Homeland Security
DHS Directives System
Directive Number: 139-08
Revision Number: 00
Issue Date: 1/15/2025
Certified Current Date: 1/15/2025

ARTIFICIAL INTELLIGENCE USE AND ACQUISITION

I. Purpose

This Directive establishes Department of Homeland Security (DHS) policy for the use and acquisition of Artificial Intelligence (AI).[1] The purpose is to advance AI innovation and governance while managing risks from the use of AI, particularly those affecting the safety or rights of individuals. Use of AI at DHS encompasses planning, designing, developing, deploying, and operating systems, services, techniques, software, and hardware by or on behalf of DHS. Use of AI at DHS may involve acquisition of AI by or on behalf of DHS by contract or other authorized procurement methods or agreements, including AI use incidental to contract performance. Acquisition of AI by or on behalf of DHS often requires development of specifications for technical requirements and development of such specifications are considered part of use of AI at DHS.

II. Scope

This Directive applies throughout DHS and to Federal, State, Local, Tribal, and Territorial government, non-U.S. government, and international entities operated by or on behalf of DHS. This Directive covers all use of AI at DHS, including AI used by elements of the Intelligence Community (IC) or as a component of a National Security System (NSS), and AI that is planned, designed, developed, deployed, operated, obtained, or procured by or on behalf of DHS. This Directive supersedes Policy Statement 139-06 *Acquisition and Use of Artificial Intelligence and Machine Learning Technologies by DHS Components*. This Directive does not apply to the DHS Office of Inspector General. This Directive does not address acquisition beyond specifications for technical requirements for acquiring AI; acquisition generally is governed by existing policy, procedures, and processes, such as DHS Directive 102-01 *Acquisition Management Directive*.

III. Authorities

A. Section 7224 in Subtitle B “Advancing American AI Act” of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 (Pub. L. 117-263, § 7224) (codified at 40 U.S.C. § 11301 note).

[1] For purposes of this Directive, AI encompasses the definitions of that term in Section 238(g) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232; 10 U.S.C. 4061 note prec.) and Section 5002 of the National Artificial Intelligence Initiative Act of 2020 (15 U.S.C. 9401).

B. Section 104 of the AI in Government Act of 2020 (Pub. L. 116-260, div. U, title 1) (codified at 40 U.S.C. § 11301 note).

C. Section 5002 of the National Artificial Intelligence Initiative Act of 2020 (15 U.S.C. § 9401).

D. Section 238(g) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232, § 238(g)) (codified at 10 U.S.C. § 4061 note prec.).

E. Section 6702 of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 (Pub. L. 117-263, § 6702) (codified at 50 U.S.C. § 3334m)

F. Executive Order 14110, *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, October 30, 2023.

G. Executive Order 14091, *Further Advancing Racial Equity and Support for Underserved Communities Through the Federal Government,* February 16, 2023.

H. Executive Order 14058, *Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government*, December 13, 2021.

I. Executive Order 13960, *Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government*, December 8, 2020.

J. Executive Order 13859, *Maintaining American Leadership in Artificial Intelligence*, February 11, 2019.

K. Office of Management and Budget, Memorandum M-24-10 *Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence,* March 28, 2024.

L. Office of Management and Budget, Memorandum M-24-18 *Advancing the Responsible Acquisition of Artificial Intelligence in Government,* September 24, 2024.

M. National Security Memorandum-25 *Advancing the United States' Leadership in Artificial Intelligence; Harnessing Artificial Intelligence to Fulfill National Security Objectives; and Fostering the Safety, Security, and Trustworthiness of Artificial Intelligence*, October 24, 2024.

N. DHS Directive 071-01, *DHS Leadership Forums,* June 30, 2015.

O. DHS Instruction 071-01-01, *DHS Artificial Intelligence Governance Board*

P. DHS Delegation 04000, *Delegation to the Chief Information Officer*

Q. DHS Designation 00-04007, *Designation of the Chief Information Officer to Serve as the Chief Artificial Intelligence Officer*

IV. Responsibilities

A. ***DHS Chief AI Officer (DHS CAIO)*** leads and coordinates, on behalf of the Secretary of Homeland Security, the use of AI at DHS, risk management from that use, and promotion of AI innovation across the Department. The DHS CAIO is responsible for leading governance and oversight structures and processes, as well as setting strategic priorities for AI deployments across the Department. The DHS CAIO also collaborates with appropriate Offices, Components, and governance groups to create and maintain a comprehensive set of policies that implement this Directive and other related DHS policies, guidelines, and processes. The DHS CAIO provides oversight, on behalf of the Department, of the comprehensive set of policy requirements implementing this Directive when the DHS CAIO fulfills such oversight through the AI Council. Per Delegation 04000 and Designation 00-04007, the DHS CAIO is the DHS Chief Information Officer (DHS CIO) or serves within the Office of the DHS CIO. As such, the DHS CAIO's responsibilities are fulfilled by the DHS CIO or in coordination with and under the direction of the DHS CIO.

B. ***DHS Chief Information Officer (DHS CIO)*** oversees AI and related infrastructure in support of DHS missions and activities as part of DHS CIO's approval and oversight responsibilities and authorities regarding implementation and use of information technology (IT), including AI, within the DHS IT enterprise. Among other responsibilities, the DHS CIO supports the use of AI at DHS through a DHS data management lifecycle framework and data standards and requirements; and ensures use of AI at DHS complies with relevant cybersecurity requirements and aligns with DHS's customer experience commitment.

C. ***Under Secretary for Management (USM)*** is the Chief Acquisition Officer and is responsible for DHS-wide governance, including policy, processes, and procedures, for major and non-major acquisition programs to include acquiring AI by contract or other authorized procurement methods or agreements. The USM ensures, in collaboration with relevant DHS officials, that acquisition of AI by or on behalf of DHS complies with applicable laws and government-wide and DHS policies.

D. ***Under Secretary for Strategy, Policy, and Plans*** leads, in collaboration with the DHS CAIO, the development of Department-wide strategies, policies, and plans regarding the use of AI at DHS and coordinates all aspects of the Department's engagement in the National Security Council policy process.

E. ***Under Secretary for Science and Technology*** leads the Department's scientific, engineering, and analytical initiatives for research, development, testing, and evaluation of AI, and for assessment of technical risk of AI; coordinates the Department's technical standards development process for AI; provides enterprise oversight for testing and evaluation of AI use cases in accordance with Delegation 10003; and supports Component Senior AI Officials regarding testing and evaluation of AI use cases within Components.

F. ***DHS Chief Privacy Officer*** has primary responsibility for both DHS privacy and information disclosure policy; exercises statutory oversight to ensure the use of AI at DHS sustains, and does not erode, privacy protections for the collection, use, retention, dissemination, or disclosure of personally identifiable information (PII); and investigates causes, weighs mitigations, and oversees implementation of remediations when suspected or confirmed PII data breaches are reported.

G. ***DHS Officer for Civil Rights and Civil Liberties*** exercises statutory authority to assess the impacts of the use of AI at DHS on civil rights and civil liberties of persons; conducts compliance and oversight activities and provides policy advice across DHS to ensure such use does not diminish the civil rights and civil liberties of persons; and collaborates with the DHS CAIO and Component Senior AI Officials to support specific AI deployment.

H. ***Assistant Secretary, Office of Partnership and Engagement*** leads, in coordination with the DHS CAIO and, as appropriate, other DHS subject matter experts, partnership and engagement for the Department with the private sector; state, local, tribal and territorial (SLTT) government; academic sector; civil society organizations and other stakeholders, including underserved communities, regarding use of AI by DHS. This includes building partnerships and conducting engagement to inform policy, operational practice, innovation, and governance; while also being responsive to stakeholder concerns, as appropriate.

I. ***General Counsel*** provides legal review, guidance, and advice on applicable laws and government-wide and DHS policies for the use of AI at DHS.

J. ***Component Heads***[2] are responsible for the use of AI within their Component and ensure that use of AI at DHS by their Component is in support of authorized DHS missions and in accordance with applicable laws and government-wide and DHS policies, including this Directive. In accordance with the authority delegated in Delegation 04000, each named Component Head with delegated responsibilities in Delegation 04000 designates a Component Senior AI Official.

[2] "Component" is defined in DHS Directive 252-01.

K. ***Component Senior AI Officials (SAIOs)*** are responsible, on behalf of their respective Component Heads, for ensuring that the use of AI within their Component is: coordinated with the DHS CAIO to support the DHS CAIO's responsibilities; safe, secure, responsible, trustworthy, and human-centered in accordance with this Directive and implementing policy; and aligned with the DHS CAIO's governance and strategic priorities for AI innovation and deployment. Component SAIOs have the expertise and authority necessary to fulfill this responsibility and work in coordination with their Component's CIO, Privacy Officer or other Officer responsible for liaising with the DHS Privacy Officer, Officer responsible for liaising with the DHS Officer for Civil Rights and Civil Liberties, senior legal counsel, and SAIO within an Element of the IC as applicable. Each Component SAIO is designated with concurrence from the DHS CAIO. If a Component uses the title of "Chief AI Officer" that Officer must be the same as the Component SAIO. For Components without the requirement to designate a Senior AI Official in accordance with Delegation 04000, the DHS CAIO or designee fulfills the responsibilities of the Senior AI Official.

L. ***Under Secretary for Intelligence and Analysis (USIA)*** serves as the Chief Intelligence Officer and Senior Information Sharing and Safeguarding Executive for the Department. Per Delegation 04000, the USIA collaborates with the DHS CAIO and the DHS CIO to provide guidance and direction, as appropriate, on the use of AI by the DHS Intelligence Enterprise (IE), including the DHS elements of the IC, and AI use within the Department's secure communications and technology, including as a part of a NSS.[3] The USIA coordinates with the DHS CAIO, the Under Secretary for Strategy, Policy, and Plans, and the DHS AI Council to ensure DHS IE policy implements this Directive, government-wide national security requirements, including NSM-25, and any other government-wide policies on use of AI within the IC or as part of a NSS, to the maximum extent possible and appropriately addresses any conflicts in requirements.

M. ***Senior AI Official within a DHS Element of the Intelligence Community[4] (IC SAIO)*** is designated in accordance with section 3334m(c) of Title 50, United States Code and government-wide national security requirements, including the requirement to designate officials to provide oversight of AI activities under NSM-25 and its successor memorandums and implementing policy. The IC SAIO fulfills the duties listed in that U.S. Code section and other applicable laws and policies, and coordinates with the DHS

[3] Consistent with the definition of Intelligence Components of the Department contained in 6 U.S.C. § 101, nothing in this Directive shall affect or diminish the authority and responsibilities of the Director of National Intelligence with respect to the Coast Guard as an element of the intelligence community, as defined under 50 U.S.C § 3003.

[4] "Intelligence Community" is defined in Section 3003(4) of Title 50, United States Code.

CAIO, the USIA, and relevant Component SAIO regarding use of AI within the element.

V. Policy and Requirements

A. ***Policy*** DHS uses AI to fulfill and advance the homeland security mission.[5] Use of AI at DHS is, first and foremost, lawful, mission-appropriate, and mission-enhancing. Use of AI at DHS also is safe, secure, responsible, trustworthy, and human-centered. DHS ensures such use of AI through rigorous testing and evaluation and appropriate data and information management, as well as through compliance with this Directive and applicable laws and government-wide and DHS policies. When use of AI by DHS involves acquisition of AI by or on behalf of DHS, DHS ensures such acquisition is responsible and authorized. DHS will continue to be a leader in the use of AI, within the U.S. Government and for the people we serve.

1. Lawful and Mission-Appropriate. Use of AI at DHS complies with the Constitution and applicable laws and government-wide and DHS policies, including those protecting privacy, civil rights, and civil liberties.

2. Mission-Enhancing. Use of AI at DHS is purposeful and performance-driven to enhance the effectiveness of DHS in fulfilling the homeland security mission through operational, administrative, and support functions.

3. Safe, Secure, and Responsible Use. Use of AI at DHS identifies and appropriately addresses risks and benefits in that use of AI; protects privacy, civil rights, and civil liberties in that use of AI; and remains hardened against compromises and malicious activity. Through rigorous testing and evaluation, DHS confirms use of AI at DHS avoids improper biases, promotes equity and fair treatment, and meets established performance metrics for effectiveness, accuracy, reliability, resilience, and security, for the specific use of AI and in accordance with applicable national and international standards. DHS requires use of AI to have human oversight when the use is safety-impacting or rights-impacting or used by DHS for significant or final agency decisions or action. DHS also ensures DHS personnel using AI and/or relying on AI outputs receive training for understanding AI generally and on the specific use of AI.

4. Trustworthy Use. Use of AI at DHS is transparent and explainable to our workforce and to those that we serve. Use of AI at DHS is publicly disclosed in plain language along with any opt-out mechanisms, to the maximum extent possible, in accordance with applicable laws and government-wide and DHS policies. Use of AI at DHS is also

[5] With honor and integrity, we will safeguard the American people, our homeland, and our values.

understandable to DHS personnel and others using AI at DHS and/or directly relying on AI outputs at DHS; those outputs are traceable and auditable to the maximum extent possible against data standards and requirements.

5. Human-Centered Use. The design, development, deployment, and operation of AI at DHS considers the humans using AI on behalf of DHS, using AI to interact with DHS, and those directly impacted by AI outputs. Use of AI at DHS aligns with DHS's customer experience commitment to deliver services that are simple to use, accessible, equitable, protective, transparent, and responsive for the people we serve. DHS uses human-centered design practices, including analysis and measurement of internal and external customer experiences related to the use of AI and its impact. DHS also consults with communities and other stakeholders affected by the use of AI at DHS, especially underserved communities, and DHS incorporates their feedback, to the maximum extent practical and as appropriate.

6. Testing and Evaluation. DHS rigorously tests and evaluates AI during design, development, deployment, and operation. Testing and evaluation is a key means of validating safe, secure, responsible, trustworthy, and human-centered use of AI by DHS. Testing and evaluation for performance, including effectiveness, reliability, and accuracy, is in accordance with applicable metrics, standards, guidance, and best practices. Testing and evaluation throughout the AI's lifecycle confirms that the AI is performing as expected and there is no improper bias in its outputs, ensures proactive risk identification and mitigation, and accounts for the evolving nature of the technology and operational performance metrics. When use of AI involves acquisition of AI, requirements for acquiring the AI supports fulfilling these testing and evaluation requirements.

7. Data Management. Use of AI at DHS complies with applicable laws and government-wide and DHS policies governing data, protection of sensitive information, and Federal records management. At DHS, data collection (including acquisition), storage, access, and use (including sharing) related to the use of AI complies with standards and requirements, including those that: protect privacy, civil rights, and civil liberties; ensure security; prevent improper biases; enhance interoperability; and advance AI output traceability and auditability.

8. Responsible and Authorized Acquisition. Acquisition of AI by or on behalf of DHS aligns with the U.S. Constitution, applicable laws, and government-wide and DHS policies, including those addressing federal procurement, privacy, confidentiality, intellectual property, cybersecurity, human and civil rights, and civil liberties. When acquisition of AI by

contract and other authorized procurement methods or agreements requires development of specifications for technical requirements, those specifications sufficiently must address testing and evaluation requirements and risk management considerations and requirements regarding use of AI at DHS. Such specifications also ensure that technical requirements support transparency, performance evaluation and improvement in AI acquired, address data ownership and management, and assess environmental efficiency and sustainability.

9. Prohibited Uses. The following uses of AI at DHS and uses of associated data are prohibited:

a. Relying on outputs of AI as the sole basis for a law enforcement action (which, for purposes of this Directive, include an arrest, search, seizure, or issuing a citation but does not include a referral to secondary screening), a civil enforcement action (including issuing a fine, injunction, or similar legal penalty), or denial of government benefits;
b. Using data associated with the use of AI at DHS, or deploying AI, to make or support decisions based on the unlawful or improper consideration of race, ethnicity, gender, national origin, religion, sexual orientation, gender identity, age, nationality, medical condition, disability, emotional state, or future behavior predictions;
c. Improperly profiling, targeting, or discriminating against any individual or entity based on the individual characteristics identified above or in retaliation for exercising Constitutional rights;
d. Using AI for unlawful or improper systemic, indiscriminate, or large-scale monitoring, surveillance, or tracking of individuals;
e. Providing DHS data, or outputs from the use of AI at DHS, to third parties for uses of AI that are prohibited by applicable laws and government-wide and DHS policies, including this Directive; and
f. Other uses of AI or associated data that are prohibited by applicable laws and government-wide and DHS policies.

B. Requirements

1. Governance and Compliance. The DHS CAIO, on behalf of the Secretary and Deputy Secretary of Homeland Security and in coordination with Component Heads, Component SAIOs, and the USIA and IC SAIOs as appropriate, provides leadership and accountability for the use of AI at DHS. The DHS AI Governance Board, along with other enterprise-wide and Component-specific governance groups as applicable, provides

coordinated and collaborative governance on issues related to the use of AI at DHS. These leaders and groups support AI use and innovation through *dynamic governance* that anticipates issues and opportunities, provides proactive guidance and leadership, and promotes equity and inclusivity by ensuring a full array of stakeholders is represented in governance groups and that diverse perspectives are incorporated into decision-making processes. Dynamic governance requires *responsive compliance* that ensures continuous feedback on requirements and processes, incorporating appropriate adjustments based on that feedback and the operational or real-world context. Responsive compliance is embedded in an enterprise AI risk management framework which is used to: assess and classify the risk of each AI use case at DHS early in its life cycle; ensure ongoing, proactive risk identification and mitigation throughout the life cycle; regularly monitor and periodically or continuously test and evaluate; and provide a foundation for advice, oversight, and support from leadership and governance groups.

2. <u>AI Governance Board</u>. The DHS AI Governance Board is responsible, in collaboration with and in support of the Deputy Secretary of Homeland Security and the DHS CAIO, for coordinating and governing issues related to the use of AI within DHS, including removing barriers to the use of AI and managing its associated risks. The Board serves as the primary coordination entity among DHS officials responsible for aspects of AI adoption and risk management.

3. <u>DHS AI Council</u>. The DHS AI Council supports the AI Governance Board and the DHS CAIO in fulfilling their respective responsibilities regarding the use of AI at DHS, and performs any other responsibilities determined appropriate by the Secretary of Homeland Security. The DHS AI Council comprises the DHS CAIO as Chair, Component SAIOs designated in accordance with Delegation 04000, the DHS CIO, IC SAIOs, the DHS Chief Privacy Officer, the DHS Officer for Civil Liberties and Civil Rights, a senior official with expertise on AI testing and evaluation from the Science and Technology Directorate, and a senior official from the Office of Strategy, Policy, and Plans. The DHS AI Council presents action items to the AI Governance Board on the use of AI at DHS, including elevating such issues to the Board as necessary. The DHS AI Council supports the DHS CAIO in issuing and maintaining a comprehensive set of policy requirements governing the safe, secure, responsible, trustworthy, and human-centered use of AI at DHS.

4. <u>AI Incident Reporting and Response</u>. DHS creates and maintains reporting requirements and response procedures for incidents involving the use of AI at DHS, including incidents that may have resulted in: harm to an individual; diminished civil rights or civil liberties of an individual or group of individuals; unauthorized release of PII or other sensitive

information, or a cybersecurity breach. Procedures for managing such incidents are appropriately coordinated among relevant officials and align with and do not supersede existing incident reporting requirements, such as those related to privacy and cybersecurity incidents.

5. Implementing Policy. DHS implements this Directive through one or more DHS Instructions, along with related policies, guidelines, and processes regarding the use and acquisition of AI at DHS.

VI. Questions

Address any questions or concerns regarding this Directive to the DHS Chief AI Officer.

RANDOLPH D ALLES

Digitally signed by RANDOLPH D ALLES
Date: 2025.01.15 15:56:03 -05'00'

January 15, 2025

R.D. Alles
Deputy Under Secretary for Management

Date