Secretary

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

Homeland
Security

August 8, 2023

Policy Statement 139-06

MEMORANDUM FOR: DHS Agency and Office Leaders

FROM: Alejandro N. Mayorkas
Secretary

SUBJECT: **Acquisition and Use of Artificial Intelligence and Machine Learning Technologies by DHS Components**

I. Purpose

Artificial intelligence (AI) will drastically alter the threat landscape and greatly augment the arsenal of tools available to succeed against new and existing threats. It has the potential to improve the efficiency of DHS business and operational processes, to strengthen customer service in travel and immigration administration and to facilitate lawful trade, while helping address a range of other challenges to the DHS mission. DHS must master this technology, applying it effectively and building a world class workforce that can reap the benefits of AI, while meeting the threats posed by adversaries that wield AI. At the same time, we must also ensure that our use of AI is responsible and trustworthy, that it is rigorously tested to be effective, that it safeguards privacy, civil rights, and civil liberties while avoiding inappropriate biases, and to the extent possible, that it is transparent and explainable to those whom we serve.

This Policy Statement guides Department of Homeland Security (DHS) Operational and Support Components (hereafter referred to as "Components") and directs actions that all Components shall undertake to establish policy and practices governing the acquisition and use of Artificial Intelligence (AI) and Machine Learning (ML) technology within the Department. This Policy Statement is the initial step in the Department's implementation of Title LXXII, Subtitle B, Section 7224(b) of the Fiscal Year 2023 National Defense Authorization Act (NDAA) (Pub. L. 117-263). This Policy Statement, and the actions it directs, are in addition to my April 20, 2023, memorandum establishing a DHS Artificial Intelligence Task Force (AITF) that will advance several specific mission applications of AI/ML to effectively address many of the Department's toughest administrative and operational challenges.

II. Standards

AI and its sub-disciplines (such as ML) offer DHS advanced capabilities to inform critical missions to protect and secure our nation. These capabilities, both existing and emerging, can help the Department meet homeland security mission requirements while safeguarding privacy, civil rights, and civil liberties. The use of these capabilities will become more common as technological systems at DHS, and throughout our nation, increasingly rely on advances made in applied AI. The Department must capitalize on the advances in AI technology to further the DHS mission, while adhering to the principles, values, and policies that guide the Department.

Principles

AI technologies enhance the Department's ability to perform vital missions and to counter threats to the security of the public. As AI technology evolves and improves, the role of AI in mission activities will become more effective and prominent. Further, the Department will leverage the benefits of AI to transform how DHS delivers services, improving and enriching the public's experience when individuals engage with the Department, and strengthening customer service and efficiency in many of our mission sets. Along with the benefits, the rapid evolution of applied AI and its adoption by the Department will present new challenges. To achieve the rapid and comprehensive incorporation of AI into the larger DHS enterprise, it is imperative that our internal policies and governance keep pace with this rapid advancement to guarantee effective oversight of the acquisition and use of AI.

The policies, updated processes and procedures, and an appropriate oversight framework articulated in this Policy Statement will be driven by the following set of principles. These principles are tailored to activities enabled by AI, but they are also consistent with core values of the Department and existing governance of all technology-dependent activities within the DHS enterprise:

- 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* (December 3, 2020), with particular attention to continued Component participation in the AI Use Case Inventory process, and adherence to the Principles for Use of AI in Government, articulated in Section 3 of that Order.

- DHS will only acquire and use AI in a manner that is consistent with the Constitution and all other applicable laws and policies, including those addressing privacy, civil rights, and civil liberties, and only where AI adoption improves mission effectiveness.

- 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, sexual orientation, gender identity, age, nationality, medical condition, or disability. DHS will continually strive to minimize inappropriate bias utilizing standards required by law and policy.

- DHS, with external assistance where appropriate, will test and validate AI employed in use cases where discriminatory activity or effects may be possible, to ensure impermissible discrimination is not occurring and to aid in advancing equity and fundamentally fair treatment. DHS will also use civil rights evaluation methods, including disparate impact analysis where appropriate, to detect impermissible discriminatory treatment that may result from the use of AI in DHS processes and activities. The threshold civil rights and civil liberties compliance question for AI is whether the algorithm complies with the applicable law and policy governing the domain in which the AI is implemented.[1]

- DHS will not use AI to improperly profile, target, or to discriminate against any individual, or entity, based on the individual characteristics identified above, as reprisal or solely because of exercising their Constitutional rights. DHS will not use AI technology to enable improper systemic, indiscriminate, or large-scale monitoring, surveillance, or tracking of individuals.

- DHS will develop, adopt, and apply a suitable enterprise risk management framework approach to AI, considering existing Federal and non-governmental risk management frameworks. The DHS AI Risk Management Framework will be applied to evaluate all use cases early in their life cycle to assess risk across a broad range of Departmental and public equities, with DHS stakeholders assessing the risk of each use case. Affected stakeholders will provide advice and oversight support to higher risk use cases, as appropriate, to assist the implementers in the mitigation of the identified risks.

- DHS will protect AI technologies from cyber-attacks and malicious degradation of algorithmic functions with adherence to Federal and DHS security standards, starting from the baseline of Government and private sector best practices, and developing new methods of addressing the evolving threat. The DHS Information Technology Security Program will update and develop additional security requirements, as appropriate, to protect AI technologies against novel cybersecurity threats and risks introduced by new applications of these technologies.

[1] For example, an AI that provides data management assistance in support of law enforcement activities must comply with the legal and DHS policy standards applicable to law enforcement, including restrictions on the inappropriate consideration of the factors listed in bullet three, above. It must also be able to comply with the substantive and procedural requirements of the justice system, such as production of the information relied upon in seeking warrants or justifying investigations and arrests, and production of exculpatory materials ("Brady material"), consistent with due process protections. Those Components engaged in AI-enabled activities pursuant to Department of Defense or Intelligence Community authorities should of course comply with their respective requirements, but also seek to harmonize their Component's activities to the extent practicable with general DHS policy.

- DHS will continue to develop a workforce that understands the strengths and weaknesses of AI embedded in DHS data systems and operations, and that is aware of the benefits and risks of this technology. All DHS users of AI are charged with providing human oversight, safeguards, and, where appropriate, review and redress in AI-enabled processes implemented by DHS, to ensure these principles are applied effectively and efficiently in the design, implementation, and end uses of this technology.

Oversight

Senior leaders at all levels of DHS, including my Office and the Office of the Deputy Secretary, as well as Component and Office Leaders, are responsible for ensuring the adoption of effective and trustworthy AI at DHS. The NDAA assigns special responsibility to the Offices named in section 7224(b), but all those engaged in this effort bear this responsibility. Together we will make DHS a leader in this space.

Actions and Next Steps

The Chief Information Officer (CIO) and the Under Secretary for Science and Technology, in consultation with the Chief Procurement Officer (CPO), the Officer for Civil Rights and Civil Liberties, the Chief Privacy Officer, and the Under Secretary for Strategy, Policy, and Plans, will establish an AI Policy Working Group (AIPWG). The AIPWG shall:

- Assess the need for Components to update or revise their existing policies, procedures and processes for the responsible, ethical, and authorized acquisition and use of AI/ML technologies across the DHS enterprise;

- Compile a record of changes in policies and procedures regarding AI completed during the AIPWG's activities;

- Develop a Directive and Instruction for Departmental clearance to drive updates that require formal policy changes to proceed; and

- Following completion of the Directive and Instruction, make recommendations to my Office regarding any other changes that should be considered to ensure the development of an enduring governance policy and framework for long term, successful, responsible and trustworthy adoption of AI at DHS.

In conducting these tasks, the AIPWG is directed to engage, support, and coordinate with the AI Task Force (AITF) I established on April 20, 2023, as directed below. As the AIPWG works to effect policy change and apply oversight to all DHS AI activities, the AIPWG will consider the following:

- The factors for responsible adoption of AI specifically cited by Congress in Section 7224(a) of the FY23 NDAA, including full implementation of EO 13960, and due consideration of the recommendations of the National Security Commission on AI;

- Best practices, risk management frameworks and other comprehensive enterprise AI governance schema established by Federal and private sector organizations;

- In coordination with the Office of the General Counsel, the legal requirements impacting the use of AI for the Department;

- Applicable regulatory compliance requirements, including the Federal Policy for the Protection of Human Subjects;

- Existing policies requiring revision due to the introduction of this new technology;

- Recommendations emerging from the ongoing work of the Homeland Security Advisory Council focused on AI in response to my tasking of March 27, 2023;

- Resourcing requirements necessary to implement any recommendations or guidance;

- Initial and recurring assessments of existing and future AI-enabled systems, with appropriate provisions for research and development activities, prototyping, and trials;

- Existing approval and oversight mechanisms that apply to AI;

- Creating a foundation for effective oversight by DHS privacy and civil rights and civil liberties subject matter experts at both the Departmental and Component level; and,

- Addressing any other topics deemed necessary by the AIPWG with the concurrence of the CIO and the Under Secretary for Science and Technology.

Within two weeks of the issuance of this Policy Statement, DHS Components, in coordination with the AIPWG, shall:

- Identify a senior career employee or servicemember with appropriate technical expertise to participate in the AIPWG (this may be the same individual assigned to the AITF), including providing the items that follow:
  - an updated inventory of current use cases of AI within their respective Component;
  - an accounting of all planned use-cases of AI within their respective Component; and,
  - any existing Component-level policies or guidance concerning the use of AI.

- Ensure AI implementation follows existing applicable law and policy governing the use, acquisition, and security of AI and similar technology and is aligned with Government-wide and interagency guidance and processes.

Pending completion of the work assigned to the AIPWG, Components shall:

- Consult with the AIPWG when requested for purposes of risk assessment of particular use cases, to receive advice on mitigating identified risks (including but not limited to privacy, civil rights and civil liberties risks) and to support policy development; and

- Provide feedback to the AIPWG that assists in developing governance policy and practices that are streamlined, tailored to support Component use cases, and incorporated into and aligned with existing processes to the extent practicable.

In order to ensure maximum efficiency and cooperation between the AIPWG and the AITF, the AIPWG shall:

- Coordinate with the AITF to ensure governance policy development efforts are aligned with and support the mission-focused AI implementation led by the Task Force;

- Provide summaries of all relevant activities to AITF leadership monthly; and,

- Open any training, speaker events or workforce development opportunities sponsored by the AIPWG to AITF members and shall seek out the views of AITF members and implementers in developing acquisition, use and security policy.

III. Definitions

The term "artificial intelligence" as used in this document refers to the definition in Section 7223(3) of the NDAA (which incorporates the definition of AI in the John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, 132 Stat. 1636, 1697-98). The term "machine learning" refers to a particular artificial intelligence discipline that is the most common artificial intelligence approach at this moment in time, but "artificial intelligence" as used in this document, the NDAA for 2023, and the NDAA for 2019, are inclusive of all types of AI that may be used in DHS programs and activities.

IV. Further Implementation

Upon completion of the work of the AIPWG and the approval of a formal Directive and Instruction on AI/ML, the Department will implement any new procedures devised under the contemplated formal policy documents and implement relevant training on those procedures. The formal Directive and Instructions on AI/ML will be complete no later than 12 months after the publication of this Policy Statement (139-96). Further recommendations of the AIPWG falling outside the scope of a Directive/Instruction process shall be made to my office for consideration and future action.

Attachments:

FY23 NDAA Section 7224
FY19 NDAA Section 238(g)

Attachment

FY23 NDAA AI REQUIREMENTS LANGUAGE

SEC. 7224. PRINCIPLES AND POLICIES FOR USE OF ARTIFICIAL INTELLIGENCE

IN GOVERNMENT.

(a) Guidance.--The Director shall, when developing the guidance required under section 104(a) of the AI in Government Act of 2020 (title I of division U of Public Law 116-260), consider--

(1) the considerations and recommended practices identified by the National Security Commission on Artificial Intelligence in the report entitled ``Key Considerations for the Responsible

Development and Fielding of AI'', as updated in April 2021;

(2) the principles articulated in Executive Order 13960 (85 Fed. Reg. 78939; relating to promoting the use of trustworthy artificial intelligence in Government); and

(3) the input of--

(A) the Administrator of General Services;

(B) relevant interagency councils, such as the Federal Privacy Council, the Chief Financial Officers Council, the Chief Information Officers Council, and the Chief Data Officers Council;

(C) other governmental and nongovernmental privacy, civil rights, and civil liberties experts;

(D) academia;

(E) industry technology and data science experts; and

(F) any other individual or entity the Director determines to be appropriate.

(b) Department Policies and Processes for Procurement and Use of Artificial Intelligence-enabled systems.--Not later than 180 days after the date of enactment of this Act--

(1) the Secretary of Homeland Security, with the participation of the Chief Procurement Officer, the Chief Information Officer, the Chief Privacy Officer, and the Officer for Civil Rights and Civil Liberties of the Department and any other person determined to be relevant by the Secretary of Homeland Security, shall issue policies and procedures for the Department related to--

(A) the acquisition and use of artificial intelligence; and

(B) considerations for the risks and impacts related to artificial intelligence-enabled systems, including associated data of machine learning systems, to ensure that full

consideration is given to--

(i) the privacy, civil rights, and civil liberties impacts of artificial intelligence-enabled systems; and

(ii) security against misuse, degradation, or rending inoperable of artificial intelligence-enabled systems; and

(2) the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of the Department shall report to Congress on any additional staffing or funding resources that may be required to carry out the requirements of this subsection.

(c) Inspector General.--Not later than 180 days after the date of enactment of this Act, the Inspector General of the Department shall identify any training and investments needed to enable employees of the Office of the Inspector General to continually advance their understanding of--

(1) artificial intelligence systems;

(2) best practices for governance, oversight, and audits of the use of artificial intelligence systems; and

(3) how the Office of the Inspector General is using artificial intelligence to enhance audit and investigative capabilities, including actions to--

(A) ensure the integrity of audit and investigative results; and

(B) guard against bias in the selection and conduct of audits and investigations.

(d) Artificial Intelligence Hygiene and Protection of Government Information, Privacy, Civil Rights, and Civil Liberties.--

(1) Establishment.--Not later than 1 year after the date of enactment of this Act, the Director, in consultation with a working group consisting of members selected by the Director from

appropriate interagency councils, shall develop an initial means by which to--

(A) ensure that contracts for the acquisition of an artificial intelligence system or service--

(i) align with the guidance issued to the head of each

agency under section 104(a) of the AI in Government Act of 2020 (title I of division U of Public Law 116-260);

(ii) address protection of privacy, civil rights, and civil liberties;

(iii) address the ownership and security of data and other information created, used, processed, stored, maintained, disseminated, disclosed, or disposed of by a contractor or subcontractor on behalf of the Federal Government; and

(iv) include considerations for securing the training data, algorithms, and other components of any artificial intelligence system against misuse, unauthorized alteration, degradation, or rendering inoperable; and

(B) address any other issue or concern determined to be relevant by the Director to ensure appropriate use and protection of privacy and Government data and other information.

(2) Consultation.--In developing the considerations under paragraph (1)(A)(iv), the Director shall consult with the Secretary of Homeland Security, the Secretary of Energy, the Director of the National Institute of Standards and Technology, and the Director of National Intelligence.

(3) Review.--The Director--

(A) should continuously update the means developed under paragraph (1); and

(B) not later than 2 years after the date of enactment of this Act and not less frequently than every 2 years thereafter, shall update the means developed under paragraph (1).

(4) Briefing.--The Director shall brief the appropriate congressional committees--

(A) not later than 90 days after the date of enactment of this Act and thereafter on a quarterly basis until the Director first implements the means developed under paragraph (1); and

(B) annually thereafter on the implementation of this subsection.

(5) Sunset.--This subsection shall cease to be effective on the date that is 5 years after the date of enactment of this Act.

SEC. 7225. AGENCY INVENTORIES AND ARTIFICIAL INTELLIGENCE USE CASES.

(a) Inventory.--Not later than 60 days after the date of enactment of this Act, and continuously thereafter for a period of 5 years, the Director, in consultation with the Chief Information Officers Council, the Chief Data Officers Council, and other interagency bodies as determined to be appropriate by the Director, shall require the head of each agency to--

(1) prepare and maintain an inventory of the artificial intelligence use cases of the agency, including current and planned uses;

(2) share agency inventories with other agencies, to the extent practicable and consistent with applicable law and policy, including those concerning protection of privacy and of sensitive

law enforcement, national security, and other protected information; and

(3) make agency inventories available to the public, in a manner determined by the Director, and to the extent practicable and in accordance with applicable law and policy, including those concerning the protection of privacy and of sensitive law enforcement, national security, and other protected information.

(b) Central Inventory.--The Director is encouraged to designate a host entity and ensure the creation and maintenance of an online public directory to--

(1) make agency artificial intelligence use case information available to the public and those wishing to do business with the Federal Government; and

(2) identify common use cases across agencies.

(c) Sharing.--The sharing of agency inventories described in subsection (a)(2) may be coordinated through the Chief Information Officers Council, the Chief Data Officers Council, the Chief Financial Officers Council, the Chief Acquisition Officers Council, or other interagency bodies to improve interagency coordination and information sharing for common use cases.

(d) Department of Defense.--Nothing in this section shall apply to the Department of Defense.

SEC. 7226. RAPID PILOT, DEPLOYMENT AND SCALE OF APPLIED ARTIFICIAL

INTELLIGENCE CAPABILITIES TO DEMONSTRATE MODERNIZATION ACTIVITIES

RELATED TO USE CASES.

(a) Identification of Use Cases.--Not later than 270 days after the date of enactment of this Act, the Director, in consultation with the Chief Information Officers Council, the Chief Data Officers Council, the Chief Financial Officers Council, and other interagency bodies as determined to be appropriate by the Director, shall identify 4 new use cases for the application of artificial intelligence-enabled systems to support interagency or intra-agency modernization initiatives that require linking multiple siloed internal and external data sources, consistent with applicable laws and policies, including those relating

to the protection of privacy and of sensitive law enforcement, national security, and other protected information.

(b) Pilot Program.--

(1) Purposes.--The purposes of the pilot program under this subsection include--

(A) to enable agencies to operate across organizational boundaries, coordinating between existing established programs and silos to improve delivery of the agency mission;

(B) to demonstrate the circumstances under which artificial intelligence can be used to modernize or assist in modernizing legacy agency systems; and

(C) to leverage commercially available artificial intelligence technologies that--

(i) operate in secure cloud environments that can deploy rapidly without the need to replace existing systems; and

(ii) do not require extensive staff or training to build.

(2) Deployment and pilot.--Not later than 1 year after the date of enactment of this Act, the Director, in coordination with the heads of relevant agencies and Federal entities, including the Administrator of General Services, the Bureau of Fiscal Service of the Department of the Treasury, the Council of the Inspectors General on Integrity and Efficiency, and the Pandemic Response Accountability Committee, and other officials as the Director determines to be appropriate, shall ensure the initiation of the piloting of the 4 new artificial intelligence use case applications identified under subsection (a), leveraging commercially available technologies and systems to demonstrate scalable artificial

intelligence-enabled capabilities to support the use cases identified under subsection (a).

(3) Risk evaluation and mitigation plan.--In carrying out paragraph (2), the Director shall require the heads of agencies to--

(A) evaluate risks in utilizing artificial intelligence systems; and

(B) develop a risk mitigation plan to address those risks, including consideration of--

(i) the artificial intelligence system not performing as expected or as designed;

(ii) the quality and relevancy of the data resources used in the training of the algorithms used in an artificial intelligence system;

(iii) the processes for training and testing, evaluating, validating, and modifying an artificial intelligence system; and

(iv) the vulnerability of a utilized artificial intelligence system to unauthorized manipulation or misuse, including the use of data resources that substantially differ from the training data.

(4) Prioritization.--In carrying out paragraph (2), the Director shall prioritize modernization projects that--

(A) would benefit from commercially available privacy-preserving techniques, such as use of differential privacy, federated learning, and secure multiparty computing; and

(B) otherwise take into account considerations of civil rights and civil liberties.

(5) Privacy protections.--In carrying out paragraph (2), the Director shall require the heads of agencies to use privacy-preserving techniques when feasible, such as differential privacy, federated learning, and secure multiparty computing, to mitigate any risks to individual privacy or national security created by a project or data linkage.

(6) Use case modernization application areas.--Use case modernization application areas described in paragraph (2) shall include not less than 1 from each of the following categories:

(A) Applied artificial intelligence to drive agency productivity efficiencies in predictive supply chain and logistics, such as--

(i) predictive food demand and optimized supply;

(ii) predictive medical supplies and equipment demand and optimized supply; or

(iii) predictive logistics to accelerate disaster preparedness, response, and recovery.

(B) Applied artificial intelligence to accelerate agency investment return and address mission-oriented challenges, such as--

(i) applied artificial intelligence portfolio management for agencies;

(ii) workforce development and upskilling;

(iii) redundant and laborious analyses;

(iv) determining compliance with Government requirements, such as with Federal financial management and grants management, including implementation of chapter 64 of subtitle V of title 31, United States Code;

(v) addressing fraud, waste, and abuse in agency programs and mitigating improper payments; or

(vi) outcomes measurement to measure economic and social benefits.

(7) Requirements.--Not later than 3 years after the date of enactment of this Act, the Director, in coordination with the heads of relevant agencies and other officials as the Director determines

to be appropriate, shall establish an artificial intelligence capability within each of the 4 use case pilots under this subsection that--

(A) solves data access and usability issues with automated technology and eliminates or minimizes the need for manual data cleansing and harmonization efforts;

(B) continuously and automatically ingests data and updates domain models in near real-time to help identify new patterns and predict trends, to the extent possible, to help agency personnel to make better decisions and take faster actions;

(C) organizes data for meaningful data visualization and analysis so the Government has predictive transparency for situational awareness to improve use case outcomes;

(D) is rapidly configurable to support multiple applications and automatically adapts to dynamic conditions and evolving use case requirements, to the extent possible;

(E) enables knowledge transfer and collaboration across agencies; and

(F) preserves intellectual property rights to the data and output for benefit of the Federal Government and agencies and protects sensitive personally identifiable information.

(c) Briefing.--Not earlier than 270 days but not later than 1 year after the date of enactment of this Act, and annually thereafter for 4 years, the Director shall brief the appropriate congressional committees on the activities carried out under this section and results of those activities.

(d) Sunset.--The section shall cease to be effective on the date that is 5 years after the date of enactment of this Act.

Attachment - FY19 NDAA Section 238(g)

JOHN S. MCCAIN NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2019

SEC 238 - JOINT ARTIFICIAL INTELLIGENCE RESEARCH, DEVELOPMENT, AND TRANSITION ACTIVITIES.

(g) Artificial Intelligence Defined.--In this section, the term ``artificial intelligence'' includes the following:

(1) Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets.

(2) An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action.

(3) An artificial system designed to think or act like a human, including cognitive architectures and neural networks.

(4) A set of techniques, including machine learning, that is designed to approximate a cognitive task.

(5) An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting.