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

Homeland Security

July 16, 2024

INFORMATION

MEMORANDUM FOR THE SECRETARY

FROM: Dr. Dimitri Kusnezov
Under Secretary for
Science & Technology

Mr. Eric Hysen
Chief Information Officer
Chief Artificial Intelligence Officer

ERIC N HYSEN Digitally signed by ERIC N HYSEN Date: 2024.08.05 13:50:34 -04'00'

SUBJECT: **Artificial Intelligence Task Force (AITF) One-Year Update**

Purpose: In the Department of Homeland Security (DHS) Artificial Intelligence Task Force (ATIF) memorandum, dated April 20, 2023, you established the AITF to advance artificial intelligence across the Department. This memorandum serves as a comprehensive update on progress toward advancing Artificial Intelligence (AI) across the DHS missions 12 months after launch and outlines major deliverables in the next six months. Future updates will be provided periodically based upon notable achievements and accomplishments by the AITF.

Context and DHS Equities: The Department has publicly committed to advancing and accelerating the responsible use of AI in support of the DHS mission. Since the inception of the AITF, the release of EO 14110 "*Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*" and the OMB M-Memo "*M-24-10: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence*" have established further AI requirements for the Department and established additional guardrails to ensure safe, secure, and responsible use. Per guidance and requirements, DHS has designated a Chief AI Officer (CAIO) and chartered an AI Governance Board. DHS has also created the AI Safety and Security Board (AISSB) for critical infrastructure.

In the last 12 months, the AITF completed a discovery phase to understand the existing use of AI within the Department and opportunities enabled by new AI technologies. The AITF completed two full-day deep dive workshops with CBP and ICE to understand the needs and uses of AI in counter-Fentanyl missions and countering child sexual exploitation and abuse material (CSAM).

Additionally, the AITF created the Responsible Use Group (RUG), led by the Office for Civil Rights and Civil Liberties, to support the Department in better understanding how to mitigate concerns of inappropriate bias, equity, and privacy in AITF championed projects. The AITF will continue its work to inform additional policy guidance, risk mitigation strategies, and an enterprise AI strategy as required by the OMB M-memo.

The AITF selected and launched pilots for three Generative AI pilots across three components. The pilots were selected for advancing the use of AI in the mission space and broad applicability to the Department's mission, and other criteria. Details about the pilots and deliverables are presented below.

In March 2024, the DHS released its AI roadmap. The first comprehensive plan for AI advancement and responsible use in the Federal Government. The roadmap provides a strategic framework for DHS to plan and track the adoption and advancement of AI across the enterprise.

Under the direction of the Secretary, efforts have been underway since February to recruit and train AI talent. DHS launched the AI Corps with the goal of hiring 50 AI technical experts to further support mission and policy priorities.

The information below is a high-level summary of accomplishments, deliveries, and work completed by the AITF over the last 12 months and provides information on plans and next steps for the remainder of 2024.

Progress Report

The AITF has concluded its first year of operations, achieving significant progress in leading, coordinating, and integrating the expansion of safe, secure, and trustworthy use of AI across the Department. This progress contributes directly to enhancing national security, improving operational efficiency, and ensuring public safety. The enclosed report details the AITF's accomplishments, with a particular emphasis on the development of the DHS AI Roadmap which details next steps towards building technical infrastructure to accelerate secure AI adoption, cultivating an AI-ready workforce, ensuring the safe, secure, and trustworthy use of AI, promoting nationwide AI safety and security, and continuing to lead in AI innovation through strong and cohesive partnerships.

In March 2024, DHS released its AI Roadmap[1] for 2024 that articulated the work of the AITF in the context of the broader Department approach to AI. The roadmap identifies three lines of efforts and several workstreams under which DHS will continue to lead in the implementation of AI as well as fulfill requirements of EO 14110 and the OMB M-memo. Future coordination of AI across DHS will be led by the AI Leadership Coordination Group (AILCG) with scheduled updates to DHS leadership. The AILCG has representation across DHS to facilitate the management and implementation of AI and ensure alignment of goals and priorities.

Notable accomplishments of the AITF include:

[1] 2024 Artificial Intelligence Roadmap, Homeland Security (dhs.gov)

Continuously and responsibly pilot and implement AI technologies in DHS mission spaces

The AITF is advancing several pilot projects with various agencies using generative AI, with a focus on large language models (LLMs):

USCIS Officer Training:
U.S. Citizenship and Immigration Services (USCIS) is leveraging LLM technology to train officers involved in refugee, asylum, and international operations. The program delivers dynamic, personalized training materials that enhance understanding of policies and laws, improve decision-making accuracy, and adds additional tools that will supplement officer training with unlimited opportunities for individualized practice.

Milestone 1- Interview simulation for one refugee persona ***(Complete)***	
Objectives	**Deliverables**
Using synthetic data, create a persona synonymous with a refugee applicant reflecting a real-world example without using real data	Selected cloud environment host for pilot LLM
Determine which cloud provider can best host an "interactive" and "chat-like" interview experience	A virtual refugee persona that responds similarly in a manner like that of an actual but notional refugee applicant
Evaluate the performance of various AI models' performance during interview simulations	

Milestone 2- Develop an LLM with basic semantic search services ***(Completed)***	
Objectives	**Deliverables**
Provide Officers with feedback on legal sufficiency and adjudicative concepts during the interview process	Display questions and answers within the User Interface that directly relate to past persecution and well-founded fear of persecution so that officers can see what specific questions & responses led to validated claims
Evaluate host platform performance to determine if it can sustain supporting the large-language model during simultaneous interviews with different trainees	
Construct a virtual personalized/tailored learning experience for officers	

Milestone 3- Updating interview simulation to use with AI models ***(In-Progress)***	
Objectives	**Deliverables**
Assess AI models for interview performance	Provide a nearly identical interview experience (and results) using new AI model as achieved with previous AI model
Complete a successful transition from current AI model to new AI model	

Milestone 4- Interview simulation for one asylum persona ***(In-Progress)***

Objectives	Deliverables
Create a persona synonymous with an asylee applicant reflecting a real-world example without using real data	Provide one asylee persona (when interacted with) that provides life-like responses
Deploy an interactive minimum viable product (MVP) that closely emulates a realistic story-telling experience for USCIS personnel	Deploy a feature-rich large-language model in Cloud environment

FEMA Planning Assistant:
The Federal Emergency Management Agency (FEMA) is utilizing generative AI to help underserved communities and local governments develop hazard mitigation plans essential for eligibility under FEMA's assistance programs. The AI application will draft portions of the hazard mitigation plan so that communities have more time to focus on increasing the quality and impact of mitigation planning through public engagement and mitigation strategy deployment.

Milestone 1- Business Requirements Analysis ***(Complete)***	
Objectives	**Deliverables**
Conduct Analysis of Alternatives (AoA)	Published AoA results, down-select final AI primary model
Identify State, Local, Tribal, and Territorial (SLTT) stakeholders	Finalized stakeholder list & Integrated Project Team membership
Build project plan & identify risks/risk mitigation	Published project plan & weekly project management review (PMR)
Determine contract needs for executing technical & non-technical tasks	Task Order awarded for engineering implementation

Milestone 2- Stakeholder Engagement ***(In-Progress)***	
Objectives	**Deliverables**
Identify candidate SLTTs in Regions 2 & 6	Identified New Jersey (Region & 2) & Texas (Region 6) candidate pilot communities
Draft Use Cases for AI Pilot	
Begin collecting hazard mitigation plan requirements for AI Pilot	
Create educational workshops for participating communities	

Milestone 3- Data Collection and Preparation ***(In-Progress)***	
Objectives	**Deliverables**
Compile approved hazard mitigation plans & identify reliable data sources	Normalized data and create structured and unstructured data sets
Prepare and vectorize hazard mitigation plans	Constructed approximately 50 approved hazard mitigation plans for use in the PARC LLM

Milestone 4- GenAI Platform evaluation and deployment ***(In-Progress)***

Objectives	Deliverables
Evaluate selected model performance in new cloud environment	Produced a validated LLM evaluation framework
Complete testing of LLM evaluation tools	Conducting educational GenAI workshops with communities in NJ & TX
Establish evaluation criteria for AI models and deployment patterns	

HSI Enhanced Search and Document Comprehension:
HSI is evaluating large-language models to enhance investigative processes by semantically searching millions of documents, retrieving relevant case information, and summarizing responses to specific queries. This accelerates the detection of crucial patterns, aiding efforts against crimes like fentanyl trafficking and human trafficking.

Milestone 1- Develop an LLM with basic semantic search services ***(Completed)***	
Objectives	**Deliverables**
Define User Experience & User Interface Wireframes	Deliver a LLM API
Migrate data to servers to test vector searching	Deliver Python AI User Interface
Establish a semantic search capability	Commission a "basic" LLM service in secure HSI environment

Milestone 2- Develop semantic search and design pipeline summarization results ***(Completed)***	
Objectives	**Deliverables**
Understand how semantic search will work on Return on Investment (ROI) documents	Deliver prototype semantic search (with ROIs) in User Interface
Begin final User Interface development	Deliver prototype summarization (with ROIs) semantic search results in User Interface
	Final wireframes & design documents

Milestone 3- Deploy final User Interface (UI) in development environment ***(In-Progress)***	
Objectives	**Deliverables**
Establish an end-state architecture	Deploy feature-complete final User Interface in a developmental environment
Determine customer loading & network scale requirements	Publish results of semantic search metrics
Implement "LLM memory"	Deliver a LLM chat bot with "memory"
	Deliver an AI Model fine tuning strategy

The AITF is continuing to evaluate these pilots beyond their initial phases and is initiating additional AI projects focusing on language translation.

Build technical infrastructure to accelerate secure AI adoption throughout DHS

OCIO and S&T are set to launch infrastructure to accelerate the adoption of AI throughout DHS. The OCIO AI Sandbox will provide DHS developers access to AI tools and capabilities to assess

how AI may support their individual missions and objectives. The S&T AI Test & Evaluation (T&E) Federated Testbed will equip DHS with a comprehensive framework to test and evaluate AI systems and models to accelerate adoption. The S&T AI T&E Federated Testbed will facilitate the measurement of AI systems during their development, deployment, and operations against established standards and metrics for responsible and trustworthy AI. The physical infrastructure of the S&T Testbed, within the federated testbed framework, will provide a secure environment for the research, development, testing, and evaluation (RDT&E) of DHS AI use cases. The initial focus will be on the use cases determined to be safety and rights impacting, including on language translation. The objective is to broaden access to the Sandbox and Testbed for more DHS users within a year, incorporating evolving T&E standards tailored to the specific missions and use cases of DHS. Additionally, S&T will establish a process for the federated AI T&E Testbed to provide independent assessment services for DHS components, including initial use cases and a five-year execution plan.

Establish rigorous development, testing, and evaluation practices for AI systems

S&T formed an AI/ML Testing & Evaluation (T&E) Working Group (AITEWG) to support the development of DHS system test and evaluation processes and will release an Action Plan covering AI/ML system pilots, use cases, training, and acquisition. The AITEWG will also provide stakeholder input and review of such key areas as AL/ML-related policy, guidance, best practices, and workforce capabilities.

Hack DHS for AI Systems will launch to utilize vetted researchers for identifying cybersecurity vulnerabilities in DHS AI systems. This initiative facilitates further security enhancements to current AI pilots and overall DHS systems.

Establish safe, secure, responsible, and trustworthy use of AI

The AI Policy Working Group (AIPWG) is responsible for effecting policy change and applying oversight to DHS AI activities, as well as engaging, supporting, and coordinating with the AI Task Force. The AIPWG first convened in November 2023 per your direction in Policy Statement 139-06, *Acquisition and Use of Artificial Intelligence and Machine Learning Technologies by DHS Components*. The AIPWG formalized and expanded an existing AI work group convened in response to requirements in the NDAA FY23. Policy Statement 139-06 was an initial step in fulfilling those NDAA requirements, and the AIPWG's work carries it forward. The AITF continues to support the work of the AIPWG by providing relevant feedback based upon information gathered learnings from the last 12 months.

A key deliverable for the AIPWG is to develop, by August 2024, a DHS Directive and Instruction focused on strategic AI governance at the enterprise level. The Directive and Instruction will also be a vehicle for implementing requirements in OMB's M-24-10 memo regarding governance and oversight of AI use at DHS. The AIPWG also began assessing existing DHS policies to determine whether policies need updates or revisions to appropriately cover use and acquisition of AI at DHS.

In addition to the work underway by the AIPWG, DHS also issued two additional policies for responsible use of face recognition and Generative AI. Directive 026-11, *Use of Face Recognition and Face Capture Technologies*, and Policy Statement, 139-07 *Use of Commercial Generative Artificial Intelligence Tools* established enterprise-wide policies for the responsible use of these technologies at DHS. The AIPWG, the AITF pilots, and the RUG will continue to inform AI policy.

The RUG has hosted five (5) working groups since January 1, averaging 75 attendees, continuing to build a community of responsible use practitioners from offices with technical, advisory, and oversight responsibilities. Internal and external speakers have shared perspectives on AI oversight practices, along with policy and organizational facets of AI implementation. The RUG sponsored three small team, supporting each AITF-sponsored project. The teams comprised of experts in privacy civil rights and civil liberties, technical subjects matter experts, and legal continue to work with USCIS, ICE, and FEMA to assess the risks of the respective AI pilots, provide governance guidance. Additionally, the RUG continues to offer policy development support at both a project and enterprise level. In one instance the RUG polled Component RUG participants, using a heat map process to identify the most relevant and resonant responsible use factors drawn from OMB M-24-10, EO 14110, the NIST AI Risk Management Framework, and other key documents, to support future governance policy development.

Grow an AI-ready Workforce

Inspired by EO 14110, the DHS AI Corps was established to rapidly recruit and onboard 50 AI technology experts, including product and policy leaders and IT specialists. Modeled after the U.S. Digital Service and DHS's own Digital Service team, the AI Corps uses OPM's new direct hire authority to staff these positions. Since its launch, the AI Corps has received over 6,000 resumes and has begun selecting suitable candidates, including appointing a new Director for the AI Corps. As of July 2024, 15 AI professionals have been onboarded to the Department. Once onboarded, these experts are be deployed across various DHS components and offices, including oversight offices, as needed. The AI Corps officially launched on February 6 during the DHS AI Day event in Mountain View, CA, which was attended by over 90 individuals including technologists, industry and academia representatives, and members from DHS Components. At the event, DHS Customer Experience, USCIS, HSI, and FEMA showcased how they utilize AI to enhance their missions.

Promote Nationwide AI Safety and Security

EO 14110 tasked CISA with providing an assessment of potential risks related to the use of AI in critical infrastructure. In response, CISA assessed potential risks for the 8 CISA-managed sectors and the elections sub-sector. Completed January 29, 2024, this assessment established a foundational analysis of cross-sector AI risks into three distinct types including attacks using AI, attacks targeting AI systems, and AI design and implementation failures.

DHS was also tasked by EO 14110 to develop AI safety and security guidelines for use by critical infrastructure owners and operators. CISA drew upon insights from this cross-sector AI risk assessment to develop these guidelines, which are framed within the context of the NIST AI

Risk Management Framework. In April 2024, DHS and CISA delivered these guidelines, which were developed in coordination with the Department of Commerce, the Sector Risk Management Agencies (SRMAs) for the 16 critical infrastructure sectors, and relevant independent regulatory agencies.

Addressing Supply Chain Challenges

The AITF will continue to collaborate with CBP and other components to enhance AI/ML advancements in ongoing programs, including the Advanced Trade Analytics Platform and Entity Resolution initiatives. These efforts are aimed at addressing and improving supply chain challenges through the strategic application of AI technologies. Additionally, the task force will produce recommendations and provide support across the departments, leveraging the work of CBP to foster broader implementation and optimization of AI solutions within DHS.

Leveraging AI to Counter the Flow of Fentanyl

DHS S&T has launched, and now transitioned to HSI, tools leveraging AI concepts such as Natural Language Processing, object detection, clustering, and Bayesian models. HSI reports that these tools have increased seizures by 50% and arrests by 8% and continue to disrupt the transnational criminal network responsible for manufacturing and distribution of fentanyl and other crimes. Additionally, collaboration with CBP and industry partners led to the deployment of a prototype hybrid computed tomography/x-ray diffraction systems at the Los Angeles International mail facility. This deployment refined ML algorithms to detect fentanyl moving in legitimate stream of commerce. S&T will continue to work with all partners to build upon the success of this mission space.

Continue to Lead in AI through Strong, Cohesive Partnerships

The AITF continues to maintain robust engagement with stakeholders in the community and industry partners to learn about the latest developments in AI and to sustain strong partnerships that advance AI for both the department and the public, as set forth in the DHS AI Roadmap. The AITF continues to collaborate with leading AI developers, AI infrastructure providers, and major tech companies, as well as academic institutions like MIT, UC Berkeley, and Stanford University. The USST and CIO/CAIO actively engage with the broader community through various speaking engagements, fireside chats at major summits, and showcases such as the GovAI Summit, IRD Showcase, and UK-Bilat events. This ongoing interaction ensures that the DHS remains at the forefront of AI innovation and application.

Homeland Security Advisory Council (HSAC) Recommendations

The AITF is committed to advancing AI within the Department and incorporating the five recommendations from the Homeland Security Advisory Council (HSAC) by:

1. Establishing the AITF as the centralized body to focus on AI/ML for DHS offices and components (completed).

2. Advancing the AITF's pilots to enhance the safe and secure integration of AI technologies for the department, thereby alleviating labor-intensive tasks and supporting decision-making.
3. Continuing engagement with stakeholders and partners in both private and public forums to forge robust, private-public-academic alliances centered on mission-critical AI applications.
4. Providing robust RDT&E guidelines and recommendations to improve the procurement of off-the-shelf commercial solutions as well as the development of in-house AI models for the department's use.
5. Establishing federated test beds to equip DHS with a comprehensive RDT&E model to advance the secure and trustworthy integration and expand data lake for AI across components.

Next Milestone

As per your direction, DHS S&T and OCIO will continue to maintain the AITF. Future reports will capture notable AI efforts throughout DHS and will continue to identify opportunities to secure the supply chain and critical infrastructure, combat fentanyl and human trafficking, and accomplish other work.

OGC/Chief Counsel Coordination: Counsel for OGC-TPLD (Steve McCleary, Nicole Marson) and OGC-GLD (OCIO) (Jennifer Carlisle, Gabe Lohr) have reviewed this memo and have no comments. OGC continues to provide legal review and support as needed.

Component Coordination: This memorandum was coordinated with the following components:

PLCY: DAS Thomas McDermott, cleared 7/01/24
OGC: DCOS Thomas, cleared 6/14/24
PRIV: CPO Mason Clutter, cleared 6/14/24
CRCL: DO Peter Mina, cleared 6/14/2
CISA: ED Brandon Wales, cleared 6/17/24
ICE: OD DCOS Lesly Company, cleared 6/14/24
CBP: DCOS Steve Schorr, cleared 6/18/24
USCIS: COS Felicia Escobar-Carrillo, cleared 06/25/24
FEMA: Sr. Technical Advisor for Data & Analytics, Julie Waters, cleared 6/14/24