Homeland Security

DEPARTMENT OF HOMELAND SECURITY

ARTIFICIAL INTELLIGENCE

ROADMAP 2024

Contents

Letter from the Secretary

Artificial Intelligence may well be the most consequential technology of our time. It has the power to innovate beyond measure, and to reshape how we secure our nation and protect our communities. At the Department of Homeland Security, we embrace the responsibility to ensure that AI is developed and adopted in a way that realizes its full potential while protecting the public from any harm its irresponsible or adversarial use might cause.

DHS is at the forefront of employing AI and machine learning technologies and leads by example. With our 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. Our use of AI not only delivers real-time benefits to the public, but also fuels our strategic efforts across all areas of homeland security.

We are excited to introduce the DHS AI Roadmap. This document outlines our AI initiatives and the technology's potential across the homeland security enterprise. It is the most detailed AI plan put forward by a federal agency to date, directing our efforts to fully realize AI's potential to protect the American people and our homeland, while steadfastly protecting privacy, civil rights, and civil liberties.

This initiative aligns with President Biden's Executive Order 14110, "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," which tasks DHS with critical roles to:

- manage AI in critical infrastructure and cyberspace;
- promote the adoption of AI safety standards globally;
- reduce the potential risk of AI's use to facilitate weapons of mass destruction attacks;
- combat AI-related intellectual property theft; and,
- ensure our nation attracts talent to develop responsible AI in the United States.

Our roadmap for the coming year includes exploring new AI applications and pursuing a whole-of-government strategy for ensuring the safe, secure, and trustworthy development and use of AI. We are seeking to engage partners across the government, private sector, and academia to bolster our nation's security.

We invite you to collaborate with us in this important mission. Together, we can responsibly and ethically leverage AI to strengthen our national security, improve our operations, and provide efficient services to the public we serve.

Alejandro N. Mayorkas

Alejandro N. Mayorkas
U.S. Department of Homeland Security
Secretary

Eric Hysen

Eric Hysen
U.S. Department of Homeland Security
Chief Information Officer

Leveraging AI to Advance the DHS Mission

Committed to safeguarding the American people, our homeland and our values, DHS continues to innovate in support of its missions.

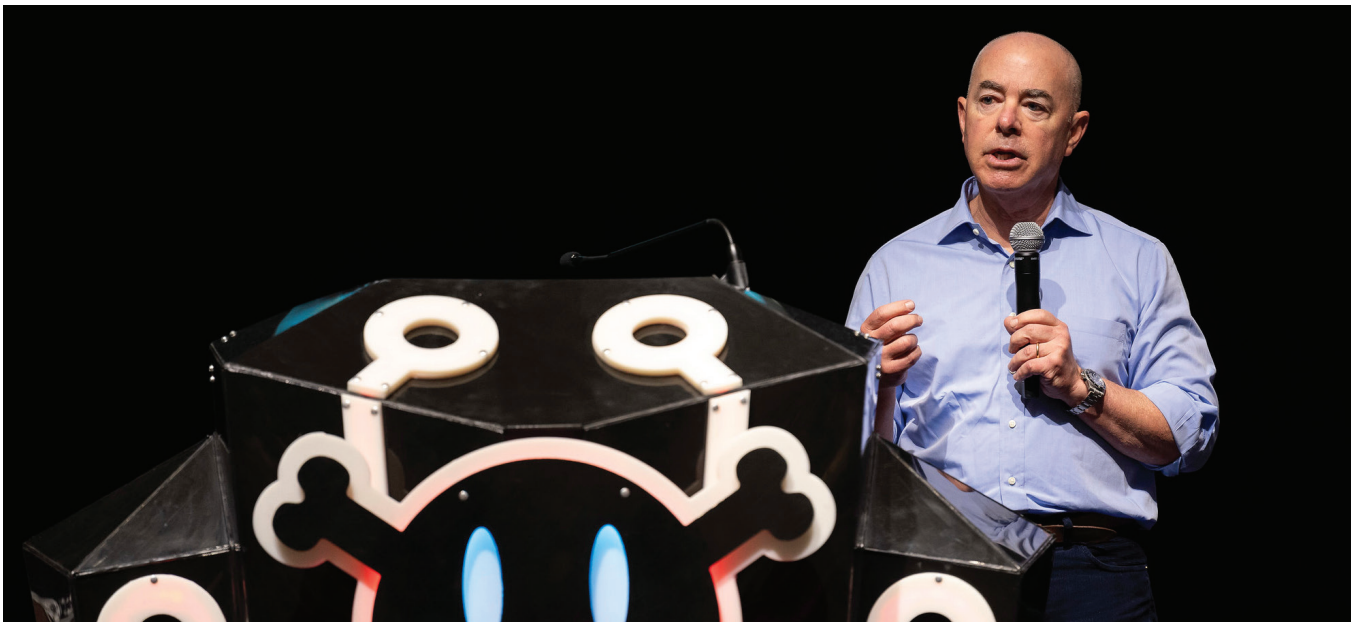
While it is now frequently in the news, the concept of AI has been around since the 1950s. Initially understood as a machine's ability to perform tasks that would have previously required human intelligence, now AI encompasses systems capable of reasoning, inference, and learning. The sophistication of AI systems has grown substantially in the past decade, and particularly in the past few years. AI systems are available to users through internet-based interfaces, increasingly integrated into software, and deployed by businesses and governments around the world.

DHS has used AI for well over a decade and continues to increase the breadth, depth, and maturity of AI's application across the Department. For example, 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. Every DHS component and office is working to meaningfully assess the potential benefits of AI to the DHS mission, and to responsibly harness its potential to further transform our operations. The Department has already published 41 different uses of AI in the AI Use Case Inventory at https://www.dhs.gov/data/AI_inventory, and the list will grow as we expand use of AI.

Some examples include:

- DHS is using AI to keep fentanyl and other dangerous drugs out of our country. The United States Customs and Border Protection (CBP) uses an ML model to identify potentially suspicious patterns in vehicle-crossing histories. CBP recently used the model to flag a car for secondary review, which yielded the discovery of over 75 kgs of drugs hidden in the automobile.
- DHS is using AI to aid our law enforcement officers in investigating heinous crimes. In 2023, the United States Immigration and Customs Enforcement Homeland Security Investigations Operation Renewed Hope identified more than 300 previously unknown victims of sexual exploitation thanks in part to an ML model that enhanced older images to provide investigators with new leads.
- DHS is using AI at the Federal Emergency Management Agency (FEMA) to more efficiently assess damage to homes, buildings, and other properties after a disaster. This approach allows FEMA inspectors the ability to look at some impacted structure damage remotely instead of conducting inspections exclusively in-person, leading to swifter delivery of disaster assistance to survivors.
- DHS is using AI to make travel safer and easier. By introducing customer-facing technologies such as Touchless Check-In at the airport, the Transportation Security Administration (TSA) provides travelers an optional way to navigate TSA security processes, check bags, and board their flights by taking just a photograph. These and other efforts are already saving time at security checkpoints and reducing physical touchpoints.

These and other current uses of AI are conducted in partnership and consultation with the Department's Offices of Privacy, Civil Rights and Civil Liberties, General Counsel, and other appropriate oversight bodies.



DHS Secretary Alejandro Mayorkas participates in a fireside chat at DEFCON 2023.

AI-driven Challenges to Homeland Security

While there are tremendous opportunities for AI to enhance the DHS mission, AI also introduces new challenges and risks. The proliferation of accessible AI tools likely will bolster our adversaries' tactics. Cyber actors use AI to develop new tools that allow them to access and compromise more victims and enable larger scale cyber-attacks that are faster, more efficient, and more evasive. Nation-states seeking to undermine trust in our government institutions, social cohesion, and democratic processes are using AI to create more believable foreign malign influence campaigns.

Of particular concern are impacts of AI attacks on critical infrastructures, which could result in nefarious actors disrupting or denying activities related to Internet of Things (IoT) technologies or networked industrial systems. Generating and passing poisoned data into a critical sensor could trigger downstream impacts, such as service disruptions or system shut-offs. AI enabled technologies are also being used to undermine the trust we place in information derived from digital content and is distinct from traditional cybersecurity threats, requiring additional research to understand and build knowledge to inform protections. Similarly, while AI has already enabled innovation in the physical and biological sciences, it also has the potential to substantially lower the barrier of entry for non-experts to design, synthesize, acquire, or use chemical, biological, radiological, or nuclear weapons.

Cyber and physical security is foundational to the safety and security of AI. DHS and the Cybersecurity and Infrastructure Security Agency in particular will continue to work to improve the nation's overall cyber resilience and to identify and manage risks associated with the misuse of AI/ML technologies. Additionally, as sector risk management agencies, TSA and the United States Coast Guard will continue to assess AI-related risks across the transportation and maritime sectors.

TSA uses new credential authentication technology to improve checkpoint screening capabilities.

Responsible Use of AI

DHS is committed to ensuring that our use of AI:

- Is responsible and trustworthy;
- is rigorously tested to be effective;
- safeguards privacy, civil rights, and civil liberties;
- avoids inappropriate biases;
- and is transparent and explainable to our workforce and to those we serve.

Where appropriate it should be interpretable to meet due process requirements in legal or administrative proceedings. DHS's use of AI should advance equity and not function in ways that amplify existing social inequalities.

DHS policy aligns with the Department's commitment to lean forward in deploying AI tools to enhance operations and lead the government in the responsible use of AI. The Department's governance and oversight of the responsible use of AI are closely coordinated, highly collaborative efforts that unite operational components and oversight offices from across DHS around the common goal of ensuring responsible use. From day one, DHS components and offices have coordinated closely with our Privacy Office, the Office for Civil Rights and Civil Liberties, the Office of the General Counsel, and additional stakeholders. These collaborations ensure compliance with all applicable laws and policies and establish clear guardrails to prohibit inappropriate use of AI/ML technologies, as well as safeguard privacy, civil rights, and civil liberties.

In 2023, DHS announced new policies and measures to promote the responsible use of AI to guide the acquisition and use of AI/ML technologies across the Department. DHS applies the principles of the blueprint for an AI Bill of Rights and will implement the National Institute of Standards and Technology's AI Risk Management Framework within the Department. As new laws and government-wide policies are developed and there are new advances in the field, we will continue to update our internal policies and procedures.

A Coordinated, Government-Wide Approach

The President's Executive Order 14110, which establishes a comprehensive strategy for AI innovation, directs DHS to partner with other federal agencies to drive a coordinated, government-wide approach. Specifically, DHS will partner with other sector risk management agencies, such as such as the National Institute of Standards and Technology, the Department of Justice, and the Department of Defense, to:

- Support sector-specific AI risk identification;
- issue guidance to agencies on how to label and authenticate their content;
- perform security reviews on AI foundational models and other measures;
- and develop guidelines, standards, and best practices for AI safety and security;

The direction provided in the Executive Order is consistent with DHS's innovative work to ensure the safe, secure, and responsible development and use of AI. DHS will continue to manage AI in critical infrastructure and cyberspace, promote the adoption of global AI safety standards, reduce the risk that AI can be used to create weapons of mass destruction and other related threats, combat AI-related intellectual property theft, and help the United States attract and retain skilled talent.

Who Does What at DHS

The **Secretary** sets the Department's AI strategy, priorities, and policies, and is the key interlocutor with the private sector, federal interagency, state officials, and key international counterparts. The Secretary represents the Department on the White House AI Council, which coordinates the activities of agencies across the federal government to implement AI policies. In April 2023, the Secretary established an AI Task Force within DHS that drives specific applications of AI to advance critical homeland security missions. The Secretary has also established and will chair a new AI Safety and Security Board (AISSB), which will provide recommendations and advice to the Secretary, the critical infrastructure community, and the broader public on the development and deployment of AI. In the Office of the Secretary, the Secretary has designated the Senior Counselor for Cybersecurity and Emerging Technology to serve as the Executive Director of the AISSB and to advise the Secretary on deploying AI and other advanced technologies to fulfill the Department's mission and support related policymaking across the Department and throughout the US government.

The Department's Chief Information Officer (CIO) serves as the designated **Chief Artificial Intelligence Officer (CAIO)**. The CAIO promotes AI innovation and responsible use across the Department and develops, in partnership with DHS offices and components, the Department's internal policies regarding its use of AI. The CAIO sets strategic priorities for AI deployments across the Department, and on behalf of the Secretary, coordinates AI-related efforts in partnerships with DHS offices and components. The CAIO also directs the Department's information security, data governance, information technology, and customer experience functions which enable DHS's use of AI.

The **Science and Technology Directorate (S&T), on behalf of the Department**, is leading AI-related research and development to provide federal, state, and local officials with cutting-edge technology and capabilities to protect the homeland. S&T leads Test & Evaluation (T&E) of AI-enabled systems, as well as the development of AI enabled T&E in partnership with the Privacy Office and operational components.

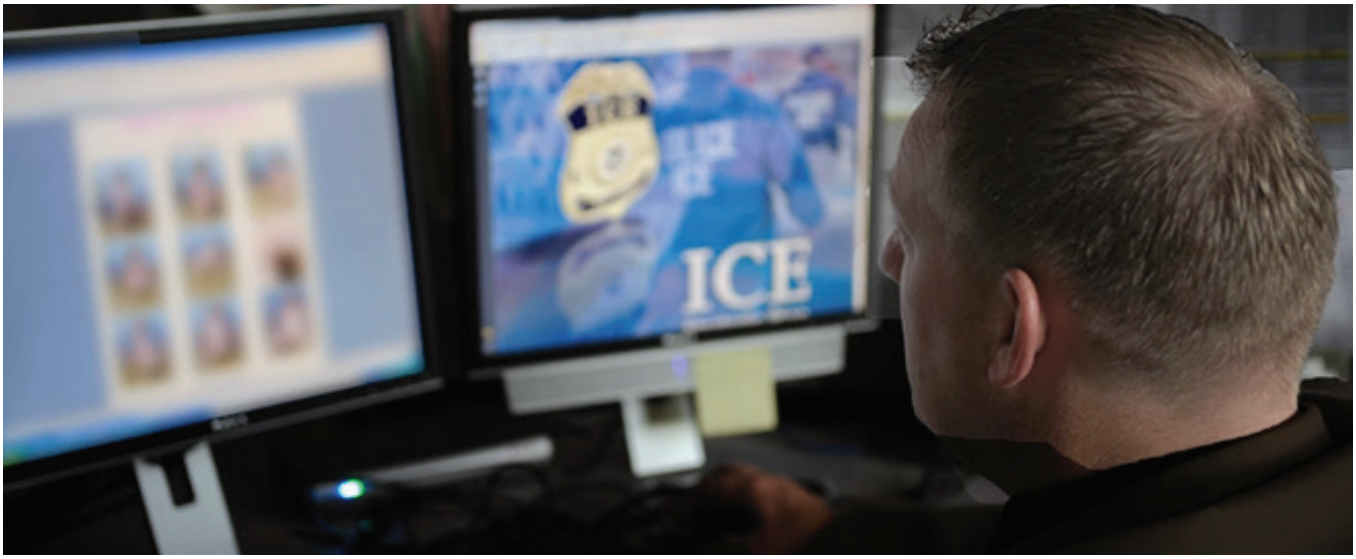
The **Office of Strategy, Policy, and Plans (Policy)** develops the Department's policy for AI, which includes overseeing the implementation of tasks directed by Executive Order 14110 and enhancing cooperation with international allies and partners on AI governance and risk mitigation. Policy supports the Secretary on the establishment and agenda of the AISSB.

The **Privacy Office (PRIV) and the Office for Civil Rights and Civil Liberties (CRCL)** oversee and provide guidance on the responsible use of AI to ensure the Department's use of AI is transparent, explainable, trustworthy, avoids inappropriate biases, and safeguards privacy, civil rights, and civil liberties. PRIV oversees DHS's use of AI to safeguard personal privacy and ensure compliance with privacy policies. CRCL works to preserve individual liberties, fairness, and equality to ensure compliance with applicable individual rights protections, including (but not limited to) due process and non-discrimination standards, and works to advance equity across all DHS AI use cases.

The **Countering Weapons of Mass Destruction (CWMD)** Office works to prevent attacks using weapons of mass destruction and other related chemical, biological, radiological, and nuclear (CBRN) threats, and leads the Department's work in identifying and reducing risks at the intersection of AI and CBRN threats. CWMD strengthens federal interagency coordination and provides direct financial aid and support to the Department's operational components and state, local, territorial, and tribal partners, and first responders.

The **Cybersecurity and Infrastructure Security Agency (CISA)** conducts cyber defense to protect against AI-enabled threats and secure AI-based software systems, as well as drive related risk reduction and resilience. CISA is also responsible

1 In 2023, CISA released a Roadmap for Artificial Intelligence to outline as set of comprehensive actions that comprise its AI mission.



HSI uses AI to investigate heinous crimes.

for communicating AI-related threat and risk information, including to critical infrastructure sectors, and responsibly integrate AI software systems across DHS.

Operational Components, including the Transportation Security Agency, United States Citizenship and Immigration Service, United States Immigration and Customs Enforcement Homeland Security Investigations, Federal Emergency Management Agency, and the United States Coast Guard, responsibly integrate AI into their operational capabilities to harness the potential of AI. These capabilities include enhanced border security, counter-fentanyl efforts, travel screening, protecting intellectual property, grant and other assistance allocation, and maritime security.

The **Office of Intelligence and Analysis** conducts and provides analysis examining how AI impacts threats, including those related to cybersecurity, foreign malign influence, and counterterrorism, to critical infrastructure and the Homeland Security mission.

The **Private Sector Office**, within the Office of Partnerships and Engagement, fosters strategic communications with businesses, trade associations, and other organizations to create stronger relationships with the Department. The Private Sector Office also helps inform the Secretary on the impacts of AI policies and regulations to the private sector, as well as promotes public-private partnerships and best practices to develop innovative approaches to homeland security challenges. The Office of Partnerships and Engagement will provide administrative support to the AISSB on behalf of the Secretary.

The **DHS AI Task Force** includes representation from across DHS components and is chaired by the Undersecretary for S&T and the CIO. The Task Force was established in April 2023 to drive specific applications of AI to advance critical homeland security missions. In collaboration with CRCL, the Task Force provides guidance, risk assessment, mitigation strategies, and oversight for the protection of individual rights. The Task Force also coordinates work to affect internal Departmental policy changes and applies oversight to all DHS AI activities.

DHS External Engagement on AI

DHS works across sectors with critical stakeholders nationwide and conducts strategic engagements and outreach with state, local, territorial, and tribal governments, elected officials, the private sector, faith-based and non-governmental organizations, academia, and communities across the nation. The Department convenes representatives of these stakeholder groups through various channels, ranging from standing advisory bodies to workshops and other targeted gatherings, to ensure the interests are represented through DHS's policy-making process. DHS also shares information and develops recommendations or guidance for increasing security and resilience.

Some of the DHS-convened groups that bring together a diverse group of stakeholders to address AI-related issues are listed below:

1. The AISSB, established by the Secretary at the direction of the President, pursuant to Executive Order 14110 Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, to bring together AI experts from the private sector, civil society, academia, and government. The purpose of the Board is to advise the Secretary, the critical infrastructure community, and the broader public on the development and deployment of AI; provide information and recommendations for improving security, resilience, and safety, including promulgating specific and actionable principles, guidelines, and best practices for the use of AI; and develop effective processes to review and respond to incidents related to the use of AI in critical infrastructure.
2. The Homeland Security Advisory Committee (HSAC) leverages the experience, expertise, and national and global connections of the HSAC membership to provide the Secretary real-time, real-world, and independent advice to support decision-making across homeland security operations. In 2023, the HSAC issued **recommendations** on AI to the Secretary, which helped inform many of the actions outlined in this roadmap.
3. DHS has existing structures in the cybersecurity domain that will be called upon to the extent that cybersecurity issues arise in the context of AI use. Chief among them is the Joint Cyber Defense Collaborative, which brings together cyber defenders from organizations worldwide to gather, analyze, and share actionable cyber risk information to enable synchronized, holistic cybersecurity planning, cyber defense, and response. In the event of a significant cyber incident either enabled by AI or on AI systems, the Cyber Safety Review Board will review what happened and produce specific recommendations to limit the likelihood or impact of such an incident in the future. Additionally, the CISA Cybersecurity Advisory Committee is comprised of experts on cybersecurity, technology, risk management, privacy, and resilience, who advise the Director of CISA on policies and programs related to CISA's mission, and specifically, how to drive adoption of secure software design practices.

Other advisory panels and committees can be found here **DHS Advisory Panels and Committees**.

Overview of the Lines of Effort

Throughout 2024, DHS will focus on the following lines of effort and associated workstreams:

1

LINE OF EFFORT

Responsibly Leverage AI to Advance Homeland Security Missions

2

LINE OF EFFORT

Promote Nationwide AI Safety and Security

3

LINE OF EFFORT

Continue to Lead in AI through Strong, Cohesive Partnerships

LINE OF EFFORT 1

Responsibly Leverage AI to Advance Homeland Security Missions While Protecting Individuals' Privacy, Civil Rights, and Civil Liberties

DHS will lead across the federal government in the responsible use of AI to secure the homeland and defend against the malicious use of AI. We will ensure that our use of AI fully respects privacy, civil rights, and civil liberties, is rigorously tested to avoid privacy harms or impermissible biases and can be explained to the people we serve.

WORKSTREAM ONE

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

DHS will use AI to support essential functions required to sustain and secure government operations. Generative AI tools, including Large Language Models (LLMs), could become integral in reducing the effort expended on business processes such as managing help desk tickets. This pragmatic approach seeks to leverage AI to streamline administrative tasks, fostering efficiency and cost-effectiveness in the day-to-day functioning of government. AI, applied strategically, serves as a transformative tool by boosting productivity and improving customer experience.

In addition to the three pilots listed below, DHS expects to initiate additional pilots across the enterprise, to include using generative AI for language translation.

2024 Goals

Officer Training Using LLMs

U.S. Citizenship and Immigration Services (USCIS) will pilot using LLMs to help train Refugee, Asylum, and International Operations Officers on how to conduct interviews with applicants for lawful immigration. USCIS will generate dynamic, personalized training materials to supplement human training that adapt to officers' specific needs to ensure the best possible knowledge and training on a wide range of current policies and laws. The pilot will help enhance officers' understanding and retention of crucial information, increase the accuracy of their decisions, and limit the need for retraining.

Planning Assistant for Resilient Communities

Federal Emergency Management Agency (FEMA) will pilot using generative AI to assist underserved communities and local governments with developing hazard mitigation plans to identify hazards, assess risks and vulnerabilities, and developing mitigation strategies. Approved mitigation plans are a requirement for local governments' eligibility for projects funded under FEMA's Hazard Mitigation Assistance program and several other types of FEMA grants for building community resilience. The pilot will specifically support state, local, territorial, and tribal governments' understanding of how to craft a plan that identifies risks and mitigation strategies and help those governments draft plan elements—from publicly-available, well-researched sources — that they can customize to meet their needs.

Enhanced Search and Document Comprehension using LLMs

Homeland Security Investigations (HSI) will pilot allowing officers to use LLMs to support their investigative processes by, (1) semantically search millions of documents, (2) retrieving relevant case documents, and (3) providing officers a summarized response to a specific query based on relevant documents. These tools should enable investigators to rapidly uncover key information and patterns. These efforts are in support of HSI's work to combat fentanyl, human trafficking, child exploitation and other criminal networks.

Transform Border Security

U.S. Customs and Border Protection (CBP) will continue to roll-out Non-Intrusive Inspection technology to make border screenings more efficient and to combat the risks associated with smuggling fentanyl and other illicit goods. Non-Intrusive Inspection is a capability used by CBP to conduct secondary screenings at border entry points via x-ray or imaging technologies, which helps CBP identify the need for any additional manual screenings. CBP will use data generated through these screenings to further enhance the imaging to more accurately detect anomalies.

Enhance Federal Cyber Defense

Cybersecurity and Infrastructure Security Agency (CISA) will assess the impact of using AI-enabled capabilities for cybersecurity vulnerability detection and remediation. CISA will deliver a report to the Secretary of Homeland Security with recommendations for actions that should be taken based on lessons learned from this assessment.

WORKSTREAM TWO

Build technical infrastructure to accelerate secure AI adoption throughout DHS

Enabling effective AI infrastructure is pivotal to the successful operation of DHS's AI ecosystem. This involves strategic considerations across:

- Data and tool management;
- storage, computing power, and networking infrastructure;
- ML operations;
- continuous integration, delivery, and monitoring;
- processes to support effective collaboration in governance and management processes;
- and implementation of privacy enhancing technologies.

Chief Data Officers (CDOs) across DHS offices and Components play a critical role in supporting the overall technical infrastructure for AI systems, which relies on high-quality, well-structured data, for reliable and efficient performance. CDOs drive data management across the Department, focusing on model training, data ontology, and privacy as the Department develops AI algorithms. CDOs also ensure precision and responsiveness in outputs, thus enhancing the overall effectiveness of AI applications.

2024 Goals

AI Sandbox

Office of Chief Information Officer, in coordination with Privacy Office, Office for Civil Rights and Civil Liberties, and Office of the General Counsel, will launch an AI Sandbox for an initial set of DHS users to experiment with implementing the responsible use of LLMs in their systems. The aim is to expand the AI Sandbox to additional DHS users within one year and integrate evolving testing and validation standards fitted to DHS mission and use cases.

Initial Operating Capability for SURVEYOR Integrated Data Environment

United States Coast Guard (USCG) will introduce the SURVEYOR Integrated Data Environment, a suite of technical components serving specific functions within an integrated cloud architecture. This enables capabilities for advanced analytics and AI, including metadata management, data access and discovery, data quality management, data transport, data processing, data storage, data visualization, data analytics, and AI/ML operations.

WORKSTREAM THREE

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

Effective development and independent evaluation processes are paramount to ensuring the responsible adoption of AI systems. A well-defined development process, including an understanding of risk assessment, documentation, and tolerance, fosters the creation of robust and reliable AI systems and helps mitigate and manage risks associated with privacy, inappropriate biases, errors, security, or unintended consequences. Comprehensive evaluation processes are equally critical in assessing the performance, compliance, fairness, transparency, and ethical implications of AI systems. This requires rigorous independent testing, validation, and continuous monitoring to build trust and accountability in AI applications.

As a part of Testing and Evaluation (T&E) needs, DHS requires comprehensive AI assurance activities to ensure the effectiveness and robustness of AI applications. These activities include benchmarking, which involves the comparison of AI models against established performance standards, as well as updates and retraining of AI models to enable the integration of new data and insights. When maintained along with testing and validation at appropriate places in an algorithm's lifecycle, AI applications can remain accurate, agile, and responsive.

To support these efforts, DHS will engage the security researcher community to help identify potential weaknesses in DHS IT systems as part of this commitment to a rigorous and secure development process. DHS will also continue to develop department-wide guidance and policies for use of AI-related technologies, as needed.

2024 Goals

AI/ML T&E Working Group

S&T will establish a Testing & Evaluation working group to support the T&E of DHS systems and publish an Action Plan for T&E of AI/ML enabled systems covering pilots and use cases, algorithm training and test data, acquisition of AI-enabled systems, use of AI for T&E, and AI-enabled adversaries.

DHS AI/ML Test Facility

S&T will create a federated AI testbed that will provide independent assessment services for DHS components and homeland security enterprise operators. Initial build out will include initial use case, testbed capability stand-up, and a five-year execution plan.

Hack DHS for AI Systems

The Chief Information Security Officer will host a HackDHS exercise to execute a crowdsourced assessment by vetted researchers on DHS IT Systems with AI. The vetted researchers will be tasked with identifying cybersecurity vulnerabilities in these systems to drive further security enhancements to DHS systems.

WORKSTREAM FOUR

Establish safe, secure, and trustworthy use of AI by DHS through robust governance and oversight policies and practices

In August 2023, Secretary Mayorkas signed DHS Policy Statement 139-06, "Acquisition and Use of Artificial Intelligence and Machine Learning Technologies by DHS Components," to define the Department's guiding principles for acquiring and responsibly using mission-enhancing AI at DHS. It includes DHS's commitment to meaningful oversight of its AI activities and safeguarding privacy, civil rights, and civil liberties. Among other commitments, DHS will not collect, use, or disseminate data used in AI activities. DHS also will not establish AI-enabled systems that make or support decisions based on the inappropriate consideration of race, ethnicity, gender, religion, sexual orientation, gender identity, age, medical condition, or disability. Furthermore, DHS will only acquire and use AI in a manner that is consistent with the U.S. Constitution and all other applicable laws and policies, especially those protecting privacy, civil rights, and civil liberties. In addition to the commitment to avoid improper profiling, targeting or discrimination, the Policy requires the establishment of an AI risk management framework suitable to the Department's AI activities.

DHS will build on this foundational policy by issuing additional policies that institutionalize responsible AI use throughout the Department and implement tailored governance approaches to different types of AI technology.

2024 Goals

DHS-wide Policy Directive

DHS will issue enterprise-wide AI policy building on the guiding principles in DHS Policy Statement 139-06. In line with the FY2023 National Defense Authorization Act, the policy will address the acquisition and use of AI; considerations for risks; privacy, civil rights, and civil liberties impacts; and security against misuse, degradation, or rending inoperable of AI-enabled systems.[2]

Internal Governance

DHS will conduct assessments of new controls and how these controls balance the use of mission enhancing AI with any potential impacts on safety or rights.

Through oversight by the highest levels of the Department, DHS will ensure all strategies and Departmental guidance are consistent with Administration policy concerning managing risks in procurement and reducing barriers to responsible use.

2 Title LXXII, Subtitle B, Section 7224(b) of the Fiscal Year 2023 National Defense Authorization Act (NDAA) (Pub. L 117-263)

WORKSTREAM FIVE

Grow an AI-ready workforce through AI literacy for all employees, programs to attract, retain, and develop AI experts, support teams, & sustaining partnerships

DHS will direct resources toward initiatives that attract, recruit, develop, and retain talent with technical skill sets to drive oversight and integration of AI capabilities. The Department will encourage interdisciplinary collaboration and forming cross-functional teams that include AI experts alongside other subject matter experts to enhance problem-solving capabilities and ensure that AI is effectively and responsibly integrated into operational and oversight processes.

DHS will also prioritize continuous training for employees to expand AI-related skill sets. In late 2023, the Department issued a policy to enable and encourage DHS personnel to responsibly use certain commercial products to harness the benefits of generative AI and ensure they can adapt to the future of work. By early 2024, hundreds of employees had taken training to use generative AI responsibly in some aspects of their daily work. These trainings are the forerunner of a larger effort to upskill our workforce over the course of the year.

DHS also plans to integrate more technical personnel into leadership and decision-making roles to achieve necessary development and retainment goals, and to AIcultivate a culture of innovation that effectively integrates data, analytics, and AI capabilities. DHS will create flexible service structures, reward diverse career paths, and foster a culture of continuous learning, to include leadership training and adaptability.

2024 Goals

AI Corps

In February 2024, DHS launched a first-of-its-kind initiative to hire 50 AI experts this year using new direct-hire authority for AI talent. The Department will deploy successful candidates to this DHS AI Corps across the Department to support mission needs and fill key roles, including in the oversight offices.

Department-wide Training

DHS will grow the number of employees across the Department who are trained and approved to leverage conditionally approved commercial generative AI tools for aspects of their work.

DHS S&T will publish recommendations for updating future DHS-wide tiered AI training content and delivery approaches, in line with the AI Training Act. The Act requires that the federal workforce has knowledge of the capabilities and risks associated with AI.

DHS will expand education for its governance and oversight personnel to understand AI's technical and operational architecture, as well as policies and standards governing the development and use of AI.

Data Analytics and AI Competencies aligned with Department of Defense Cyber Workforce
The USCG will continue to mature its data and AI workforce by establishing five new military competencies in the field of data, analytics, and AI. The USCG will implement training for each new competency to upskill our workforce and better align personnel to emerging service demands. Finally, the USCG will conduct data and AI literacy programs at various levels throughout the service to increase cooperation and the effective use of AI capacity.

LINE OF EFFORT 2

Promote Nationwide AI Safety and Security

Advances in AI will revolutionize the delivery of essential goods and services upon which Americans rely. AI can create tremendous efficiencies and benefits for citizens, but it will also present new and novel risks. To protect national networks and critical infrastructure, the President has directed DHS to take several steps to help govern the safe and responsible development, and use of AI.

WORKSTREAM ONE

Protect AI systems from cybersecurity threats and guard against AI-enabled cyberattacks

DHS will capitalize on AI's potential to improve cyber defense. Within DHS, we will conduct operational tests to evaluate AI-enabled vulnerability discovery and remediation techniques for federal civilian government systems. Furthermore, CISA is already actively leveraging ML tools for threat detection and prevention. CISA will continue partnering with government and private sector experts to assess and counter the use of AI by malicious actors targeting government and critical infrastructure systems. For example, in November 2023, CISA and the United Kingdom's National Cyber Security Centre published Guidelines for Secure AI System Development, co-sealed by 23 domestic and international cybersecurity organizations. It provides essential recommendations for AI system development and emphasizes the importance of adhering to Secure by Design principles.

2024 Goals

Actionable Risk Management Guidance

CISA will publish guidance on AI security in partnership with international partners and other federal entities, such as the National Institute of Standards and Technology (NIST), the National Security Agency, and the Federal Bureau of Investigation. Its ongoing AI security guidance will provide suggestions and mitigations to help critical infrastructure owners and operators, data scientists, developers, managers, decision-makers, and risk owners make informed decisions. The guidance will highlight decisions related to the secure design, model development, system development, deployment, operation, and use of AI systems. CISA will provide recommendations on external testing for AI to the Office of Management and Budget for incorporation into guidance for the federal government. CISA will also work with NIST to develop best practices and guidance for AI red teaming, with a focus on the cybersecurity red teaming of AI systems.

WORKSTREAM TWO

Combat AI's use to generate CSAM, CBRN threat information, and other material that threatens homeland security

The advent of AI may make it easier for malicious actors to develop weapons of mass destruction and other related threats. Of particular concern is the risk of AI-enabled misuse of synthetic nucleic acids to create biological weapons. Also, AI can be used to generate child sexual abuse material (CSAM), either in the form of computer-generated imagery or of benign imagery of real children that has been digitally manipulated to make it appear as though the children are engaged in sexually explicit conduct.

To mitigate these risks, DHS will work with the White House Office of Science & Technology Policy (OSTP) and other relevant US government agencies to evaluate the potential for AI to lower the barriers to entry for developing weapons of mass destruction and chemical, biological, radiological, or nuclear (CBRN) threats. Furthermore, DHS will develop a framework to evaluate and stress test synthetic-nucleic acid screening, build a culture of shared expectations for third parties that audit AI systems for misuse, and prevent the risk of abuse and proliferation by malicious actors. DHS will work to combat the use of AI to produce and distribute CSAM, particularly in the forms of new AI-generated content and in the manipulation of benign images of children.

2024 Goals

CBRN Report and Framework

Countering Weapons of Mass Destruction Office (CWMD) will draft a report for the Secretary to deliver to the President on AI CBRN Risks and Benefits as required by Executive Order 14110 section 4.4(a)(i).

CWMD will develop a framework to stress-test the OSTP developed system for screening synthetic nucleic acid.

CWMD works with NFL, Nevada, and Las Vegas partners to secure Super Bowl LVIII.

WORKSTREAM THREE

Assist AI developers in combating AI-related IP theft, developers and copyright holders in mitigating AI-related IP risks, and agencies in labeling and authenticating official digital content

Protecting intellectual property (IP) is critical to the United States' global competitiveness; IP theft threatens businesses and jobs and negatively affects our national security. To address this challenge, DHS, through the National Intellectual Property Rights Coordination Center, will create a program to help AI developers mitigate AI-related IP risks by leveraging Homeland Security Investigations (HSI), law enforcement, and industry partnerships.

2024 Goals

Managing IP Theft Risk

HSI will deploy a training and outreach program to educate industry on AI-related IP threats as well as best practices, protection, and mitigation strategies.

HSI will launch a program to assist AI developers in identifying AI-related IP theft risks.

WORKSTREAM FOUR

Mitigate AI risks and threats to critical infrastructure by providing guidelines for secure AI use

DHS will work with stakeholders inside and outside of government to develop AI safety and security guidance for use by critical infrastructure owners and operators. CISA, TSA, and USCG are assessing potential risks related to the use of AI in critical infrastructure sectors, including ways in which deploying AI may result in failures, physical attacks, and cyberattacks. We will take a global, harmonized approach by working with international partners on these guidelines.

2024 Goals

Sector Risk Assessments

CISA will build on its work completing Critical Infrastructure Risk Assessments for AI across all 16 sector risk management agencies. Based on these assessments, CISA will highlight common risk categories and mitigation strategies, then use the analysis to inform future planning efforts and advise critical infrastructure owners and operators.

DHS, led by CISA, will incorporate the National Institute of Standards and Technology AI Risk Management Framework and other relevant AI security guidance into safety and security guidelines for critical infrastructure owners and operators.

WORKSTREAM FIVE

Establish the AI Safety and Security Board as an authoritative public-private partnership to enable the safe and secure use of AI in the delivery of critical services to Americans

At the direction of the President, the Secretary will establish and chair the Artificial Intelligence Safety and Security Board (AISSB) to support the responsible development and deployment of AI. The AISSB will bring together preeminent industry experts from the AI technology industry; critical infrastructure owners and operators; federal, state, and local governments; academia and research organizations; and non-profit organizations.

2024 Goals

Establish and Commence the Work of the AISSB

DHS will stand-up and convene the AISSB to provide advice, information, and recommendations to the Secretary, the critical infrastructure community, and the broader public on the development and deployment of AI. The AISSB will begin issuing its recommendations and public facing guidance on improving the security, resilience, and safety of AI usage in critical infrastructure.

WORKSTREAM SIX

Streamline visa processes to recruit more AI talent to the United States

Attracting and cultivating diverse talent in AI and other emerging technologies is critical to the global competitiveness of the United States. DHS will streamline processing times of petitions and applications for noncitizens who seek to travel to the United States to work on, study, or conduct research in AI or other critical and emerging technologies. DHS will also clarify and modernize immigration pathways for such experts, including those for O-1A and EB-1 noncitizens of extraordinary ability; EB-2 advanced-degree holders and noncitizens of exceptional ability; and startup founders using the International Entrepreneur Rule.

DHS has already advanced policy consistent with direction in the Executive Order. In October, 2023, USCIS published a Notice of Proposed Rulemaking to modernize the H-1B visa specialty occupation worker program and enhance its integrity and usage, and in February 2024, certain provisions were finalized in an H-1B registration rule. USCIS continues to work on rulemaking to enhance the process for noncitizens, including experts in AI and other critical and emerging technologies, as well as their spouses, dependents, and children, to adjust their status to lawful permanent residents. On September, 2023, USCIS clarified guidance on evidence for EB-1 individuals of extraordinary ability or outstanding professors or researchers.

2024 Goals

USCIS Enhancements

USCIS will publish updated policy guidance for international students, including how F-1 visa holding students seeking an extension of optional practical training OPT based on their degree in a science, technology, engineering, and mathematics (STEM) field may be employed by startup companies.

USCIS will publish a data report, consistent with Executive Order 14110 section 5.1(g)(iii), that shows increased utilization of the O-1 and EB-2 pathways by global STEM talent.

LINE OF EFFORT 3

Continue to Lead in AI through Strong, Cohesive Partnerships

Expanding strategic partnerships through collaboration with industry leaders, research institutions, other government agencies and non-government organizations, and international partners can provide DHS with access to cutting-edge technologies, diverse expertise, and a broader knowledge base. This exchange of knowledge accelerates the development and deployment of AI solutions tailored to the unique challenges faced by the DHS. By fostering a collaborative ecosystem, DHS can harness the collective intelligence of the broader AI community, resulting in more robust, adaptable, and innovative solutions.

WORKSTREAM ONE

Foster strong relationships with private sector, academia, SLTT governments, international partners, non-government organizations, and thought leaders to advance these objectives

DHS will continue to build on its work through industry collaboration and coordination, and through bilateral engagement within and outside already established channels. In particular, the Secretary will continue to share the Department's vision and mission related to AI with international counterparts and in forums such as the Munich Security Conference. Through the Private Sector Office, DHS will build on successful and widely attended stakeholder convenings to share resources and address questions. CISA, as well, will leverage existing structures to advance industry collaboration and coordination around AI security. For example, CISA will use the Information Technology Sector Coordinating Council's AI Working Group, and the Joint Cyber Defense Collaborative to catalyze focused collaboration around threats, vulnerabilities, and mitigations affecting AI systems. Across the federal government, S&T will participate in the US AI Safety Institute Consortium and manage the Department's related memoranda and agreements that define the partnerships with academia and the private sector.

WORKSTREAM TWO

Communicate DHS efforts in AI through public messaging and engagement

In line with the DHS's commitment to transparency and visibility into the Department's vision for AI and to ensuring responsible use, DHS will continue to publicly share information about its own activities and use. The information will be presented in a way that is accessible for the people it serves. DHS will share products on its public facing website (dhs.gov/ai) and on its social media channels. Additionally, the Secretary will communicate the Department's AI-related efforts through engagements with the media and across diverse audiences, ranging from critical infrastructure owners and operators to technology executives to civil society. Other DHS leaders will continue to share information broadly through DHS platforms, at industry conferences, and in media outlets.

WORKSTREAM THREE

Create transparency and build trust around DHS use of AI through engagement with oversight entities and Congress

Department leadership will continue to engage with Congress, as well as external and internal oversight entities, to provide updates on DHS's use of AI. In 2023, for example, the Chief Artificial Intelligence Officer testified before Congress on "How Federal Agencies are Harnessing Artificial Intelligence," and has continued to work with committees of jurisdiction across the Senate and the House to describe DHS's planning efforts for both future AI use and protecting against AI-enabled threats.

DHS, and Office for Civil Rights and Civil Liberties in particular, will collaborate with federal civil rights offices and independent regulatory agencies to comprehensively use their respective authorities and offices to prevent and address discrimination in the use of automated systems, including algorithmic discrimination. Among other actions, DHS will join the interagency *Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems* affirming the Department's responsible use of AI and commitment to ensuring federally conducted and assisted activities comply with civil rights law and policy, as applicable.

WORKSTREAM FOUR

Engage with communities, advocates, and partners to demonstrate responsible AI use

The Privacy Office, Office for Civil Rights and Civil Liberties, and Office of Partnerships and Engagement will facilitate Department outreach to communities, advocates, and partners to receive feedback from privacy, civil rights, and civil liberties experts, and communities potentially impacted by the Department's use of AI. This engagement will be used to inform the development of AI that supports DHS missions, specifically to help build in protections of privacy, individual rights, and fundamental fairness. DHS will continue to host convenings with privacy, civil rights, and civil liberties advocates to share information about DHS's work.

Glossary

The definitions of the following terms referenced in this document are drawn from Executive Order 14110, unless otherwise specified.

ARTIFICIAL INTELLIGENCE (AI)

The term "Artificial intelligence" (AI) meets the definition spelled out in 15 U.S.C. 9401(3): a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.

AI MODEL

The term "AI model" means a component of an information system that implements AI technology and uses computational, statistical, or machine-learning techniques to produce outputs from a given set of inputs.

AI SYSTEMS

The term "AI systems" means any data system, software, hardware, application, tool, or utility that operates in whole or in part using AI.

GENERATIVE AI

The term "generative AI" (or, GenAI) means the class of AI models that emulate the structure and characteristics of input data in order to generate derived synthetic content. This can include images, videos, audio, text, and other digital content.

INTERNET OF THINGS

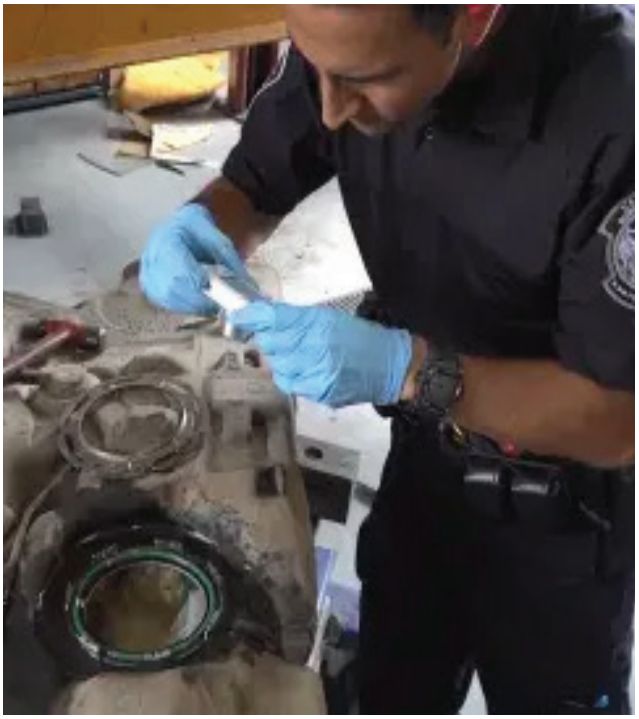
IoT (as defined by DHS) refers to the connection of systems and devices with primarily physical purposes (e.g. sensing, heating/cooling, lighting, motor actuation, transportation) to information networks – including the Internet – via interoperable protocols, often built into embedded systems.

LARGE LANGUAGE MODEL

According to the Department, the term large language model (LLM) means a type of machine learning model that is trained on a broad set of general domain data for the purpose of using that model as an architecture on which to build multiple specialized AI applications.

MACHINE LEARNING

The term "machine learning" (as defined by DHS) means a set of techniques that can be used to train AI algorithms to improve performance at a task based on data.



CBP uses AI to keep fentanyl and other drugs out of the country.

Homeland Security

DEPARTMENT OF HOMELAND SECURITY **ARTIFICIAL INTELLIGENCE**

ROADMAP 2024