U.S. DEPARTMENT OF HOMELAND SECURITY

ARTIFICIAL INTELLIGENCE STRATEGY

December 3, 2020

Vision: *The Department of Homeland Security will enhance its capability to safeguard the American people, our homeland, and our values through the responsible integration of artificial intelligence (AI) into the Department's activities and by mitigating new risks posed by AI.*

Table of Contents

INTRODUCTION

Artificial Intelligence (AI) refers to automated, machine-based technologies with at least some capacity for self-governance that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. The increased use of AI is inevitable as part of the ongoing global race to leverage new technologies for competitive advantages by nations and to increase economic prosperity by private sector entities. Use of AI can transform global economies, effect U.S. national security, and impact American citizens in their daily lives. The potential impact of AI also extends to critical infrastructure sectors like manufacturing, financial services, transportation, healthcare, energy, and food and agriculture.

AI presents opportunities for the Department of Homeland Security (DHS) to more effectively or efficiently accomplish our mission to secure the homeland. Yet with increased use of AI systems across the homeland security enterprise, comes increased risk. These risks include compromised or poorly designed AI systems, as well as adversarial use of AI technologies by unfriendly nations or criminals to increase their malicious capabilities. The potential impacts from AI on the security of the homeland and upon our Department's operational activities—both positive and negative—make it imperative for DHS to take a proactive role in the use of AI systems and to contribute to the national conversation on the secure use of this transformative technology. Therefore, DHS must act to ensure it is positioned to capitalize on the opportunities and benefits of AI, while constantly evaluating risks associated with the use of AI across the homeland security enterprise and the adversarial use of AI to cause us harm.

AI offers rich opportunities to improve the way we accomplish our mission across DHS Components. Efforts to secure the border, identify and interdict criminal actors, and secure cyberspace will be aided by use of AI systems. This strategy therefore seeks to prioritize the responsible use of AI by DHS while also mitigating AI-related risks to our homeland, citizens, and values.

While we work to reap the potential benefits of AI as a Department, we must also ensure that our use of AI comports with best practices and promotes trust and confidence of the public and of our domestic and international partners. DHS will be guided by the principles set forth in Executive Order 13690, *Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government* (December 3, 2020). Trust in the Department's expertise to identify and mitigate security risks and in its responsible use of its own AI systems is at the core of DHS's future success and leadership in AI. Furthermore, public input, especially in those instances where AI uses sensitive personal information, will improve the Department's accountability and increase the trust and confidence of the American people.

However, we must also be aware of other risks associated with the use of AI by partners and stakeholders across the homeland security enterprise, and the risks associated with the malicious use of AI to threaten the homeland. Potential adversarial use of AI will continue to evolve at pace with the development of the technology. Adversaries can increasingly use AI-enabled systems to exploit or overcome security measures currently in place at our physical borders including at ports-of-entry, in cyberspace, in election systems, and beyond. DHS will work to make our nation more secure and resilient against the malicious use of AI and other emerging technologies by other nations and by criminals.

DHS will take a proactive role in the ongoing national conversation on AI by issuing this strategy and through the development of a subsequent implementation plan. The strategy sets out five goals to govern the Department's approach to successfully integrating AI into our mission in a responsible and trustworthy manner and successfully mitigating risks associated with AI across the homeland security enterprise.

DHS AI Goals

1. *Assess Potential Impact of AI on the Homeland Security Enterprise*
2. *Invest in DHS AI Capabilities*
3. *Mitigate AI Risks to the Department and to the Homeland*
4. *Develop a DHS AI Workforce*
5. *Improve Public Trust and Engagement*

Figure 1. DHS AI Goals

These concrete and achievable goals for DHS are consistent with the Department's strategic vision which is set out below and is grounded in a risk-informed model that fosters accountability, transparency, trust, and security.

Strategic Vision

Our strategic vision is that DHS will become a global leader in policy development, governance, and the use of AI systems as we lead national efforts to mitigate against institutional and enterprise risks posed by AI. DHS Components will take actions to identify opportunities for purpose-driven and tailored AI solutions for mission enhancement and continuously identify risks when considering the use case for a new AI system or when evaluating an existing system. DHS will simultaneously engage with external partners, including the public, to effectively communicate its AI policies and to grow and maintain an expert workforce to lead the responsible and accountable use of AI throughout the system's life cycle.

In furtherance of its mission, DHS will strive for the highest standards of transparency, accountability, and public outreach. Public trust in the Department's expertise to operate its own AI systems and to identify and mitigate security risks is at the core of DHS's future success and leadership in AI. Innovation and growth in AI should therefore be prioritized, in all instances, in accordance with fundamental rules and best practices to address the creation, acquisition, privacy, integrity, security, quality, and use of AI systems and any associated data sources.

We will remain always vigilant to emerging AI risks in carrying out the vital missions of protecting the American people as the Department becomes a leading practitioner of AI. DHS will develop comprehensive risk assessments and mitigation measures to ensure the continued success of the homeland security mission and protection against adversarial use of AI. DHS will leverage existing and new partnerships across the AI and homeland security communities to inform and manage AI risks to the homeland.

DHS Approach

DHS has a responsibility to the American people to innovate in support of its mission and to do so responsibly and deliberately. AI has already emerged as a technology and is increasingly ubiquitous in applications used every day across private sector, academia, and the U.S. Government. As is the case across the Federal Government, DHS is currently deploying and operating various AI systems.   AI brings tremendous potential to improve processes that yield increased efficiency and effectiveness across the public and private sectors alike. As with any technology, however, opportunities for innovation come with risks.

For DHS to accomplish our mission to safeguard the American people, our homeland, and our values, we must use AI consistent with law and respectful of those values we seek to safeguard. We must ensure, for example, that DHS Components have measures in place to increase transparency, accountability, and to regularly monitor AI systems for potential bias and error.

The integration of AI into the current technology landscape combined with the rapid pace of development led the White House to develop EO 13960. That executive order sets forth the principles that will guide the use of AI across the Federal Government and by the Department. The principles were designed to provide a framework for DHS and other federal agencies to consider when weighing the adoption of AI solutions. This DHS AI Strategy is guided by and builds upon the principles in the EO. The DHS AI Strategy seeks to position the Department to take advantage of creative and innovative AI solutions consistent with the principles in EO 13960.

While the principles of EO 13960 will serve as our foundation, this strategy sets forth broader strategic goals that will prepare the Department to be a responsible and trustworthy user of AI and to secure the homeland against risks presented by AI technology and by adversarial use of AI. AI has shown great promise at DHS to enhance a variety of missions such as cybersecurity protections, law enforcement investigations, and a range of other operational efficiencies. Currently, however, these DHS AI systems operate in the absence of a unified, enterprise-level strategic approach to AI usage and investment.

The first goal of this strategy calls for the Department to take a comprehensive, wholistic, and strategic look at AI in terms of the potential impacts—positive and negative—that it can have across our mission set. Such an assessment, leveraging expertise inside and outside the

Department, will better position DHS to effectively make informed decisions about its AI-related efforts. Goal 2 then focuses on the need for strategic investment by DHS in AI, including an assessment of current capabilities, a Department-wide effort to invest in core infrastructure needed to run advanced AI algorithms securely and efficiently, consideration of realistic research and development opportunities, and associated budget priorities. The objectives under Goal 2 will drive a concentrated effort to strategically position DHS to take advantage of the opportunities present by AI.

As previously noted, AI also presents risks and challenges for DHS in addition to significant opportunities. As recognized in EO 13960, questions around the governance of AI systems remains a persistent problem across academia, legal circles, and the AI user community. Goal 3 identifies a series of objectives to ensure that DHS implements the principles set out in EO 13960 to ensure that DHS AI systems are accurate, safe, understandable, and regularly monitored as part of a consistent approach to effective governance rather than through ad hoc DHS Component practices. Goal 3 also sets out strategic objectives to address other risks posed by reliance on AI systems across the homeland security enterprise and potential adversarial use of AI to target the homeland. Key objectives include engaging and educating key stakeholders about AI risk, supporting the development of community and international AI standards, and mitigating identified adversarial use AI risks to the homeland.

Of course, a foundation for success in meeting these first three strategic goals will be the development of a professional AI workforce supporting the homeland security mission. Goal 4 therefore focuses on the need for DHS to improve its ability to attract and retain AI professionals across disciplines as it works to improve its science, technology, engineering, and mathematics (STEM) workforce. To keep pace with the development and application of new AI systems, the Department must develop and retain an expert AI workforce within our Science & Technology Directorate (S&T) and across other DHS Components. Reflective of a national need for AI professionals in government, private industry, and academia, DHS must partner with the academic and private sectors to become a destination of choice for highly educated and highly talented STEM experts. Similarly, DHS success must be founded on engagements that will build public trust in AI generally and in DHS's use of AI particularly. Goal 5 focuses therefore sets out objectives for DHS efforts to engage and increase such trust.

DHS faces both opportunities and challenges to achieve our vision to become a leader in the trustworthy use of AI. We recognize the need to prioritize and inspire creative and innovative thinking that leads to the rapid and safe adoption of new technologies. We also recognize the need to identify and mitigate possible risks from AI by investing in our capabilities to meet those challenges. Our efforts, guided by the principles in EO 13960, will contribute to an improvement of the public's trust in the Department's ability to use AI effectively and responsibly to safeguard our homeland, our citizens, and our values.

Development and Implementation

The DHS Office of Strategy, Policy, and Plans (PLCY) led the development of this strategy in collaboration with all DHS Components. DHS will also issue a corresponding implementation plan to outline DHS Component roles, responsibilities, programs, and timelines for accomplishing these goals and objectives.

This strategy and the implementation plan will be used to harmonize and prioritize DHS AI planning, programming, budget, training, and execution activities. In addition, the Joint Requirements Council will utilize the strategy and implementation plan to support the review of capability gap analyses and requirements generated by relevant Components. PLCY will annually assess implementation of this strategy and provide a report to the Secretary. The report will include areas of success, opportunities for improvement, constraints impeding progress, and suggested adjustments to the strategy. DHS will review and assess the need to update this strategy in 2024, and periodically thereafter.

Goal One – Assess Potential Impact of AI on the Homeland Security Enterprise

The rapid development of AI and its broad applicability present opportunities for DHS to improve our mission execution but also new risks to our mission execution and risks to the homeland from increased adversary capabilities. DHS will begin by improving its strategic cooperation with interagency partners, foreign partners, academia, and the private sector to continually assess AI's impact to the DHS mission. Improved strategic cooperation will effectively position the Department to make critical and informed assessments of the impact of AI technology across its missions, both positive and negative. Such cooperation will provide the Department with broad perspectives on the most up-to-date information on the research, development, and potential applications of AI.

AI-related opportunities and risks will evolve at the pace of technological development and the Department must be positioned to act quickly to leverage new technologies. Concurrently, DHS must also counter threats such as AI-enabled computer network intrusions, threats to critical infrastructure, deep-fakes, big data processing, and misinformation campaigns. Accomplishment of this goal will create a robust and diverse understanding of opportunities and risks to the Department's mission while advancing the principles of EO 13960 domestically and internationally.

Objective 1.1: Develop Knowledge of Technical Applications of AI

DHS will partner with private sector entities, international partners, and academic institutions to survey and assess current research and publications related to AI technological developments with the goal of assessing AI impacts specific to the homeland security mission. This objective will position the Department to identify possible AI-associated opportunities and risks, and to develop mitigation measures to counter the risks.

Objective 1.2: Identify Opportunities for AI Use

DHS will identify legacy systems, processes, and mission areas to which the addition of a purpose-driven and tailored AI solution would result in increased efficiencies, optimal use of resources, and general mission enhancement across the Department. Integration of AI will be guided by the principles in EO 13960 and in accordance with Objective 3.1 below.

Objective 1.3: Identify Critical Applications and Impact of AI on U.S. Critical Infrastructure

DHS will leverage its existing authorities and relationships and examine the need for new relationships to engage the critical infrastructure community and academia to inform and study the current and future beneficial effects and risks of AI on U.S. critical infrastructure systems.

Goal Two – Invest in DHS AI Capabilities

DHS must take steps to ensure that we are able to take advantage of new AI systems and the opportunities they present. AI algorithms rely on advanced computational capabilities, secure data storage, and the infrastructure to move large amounts of data at high speeds. DHS will therefore survey existing capabilities, identify gaps, and invest in infrastructure and supporting technologies to support the large computational and data storage demands of future DHS AI systems.

Infrastructure investments shall be structured in a manner that is consistent with law and policy, particularly when such infrastructure uses, leverages, or maintains personally identifiable information (PII). Specifically, the Department will focus on high performance computing, secure cloud computing, special purpose processors, Graphics Processing Unit (GPU) capabilities, fast data connections, large data storage and computation capabilities, and improved data connections. This investment will serve as the foundation upon which future AI capabilities can be built and will give the Secretary the option to implement an AI solution to execute DHS missions.

DHS will also develop research and development priorities to determine whether and how to contribute limited departmental R&D funding to support AI systems most relevant to the homeland security enterprise. To support these objectives, DHS must relook at current and future budgets in light of the impact AI will have on DHS operations and activities. Accomplishment of this goal in the spirit of this strategy will position the Department as a Federal Government leader in AI-ready infrastructure and capabilities and contribute to public trust in the responsible use of AI consistent with Goal 5.

Objective 2.1: Survey Existing Computational and Data Storage Capabilities for Security and Storage Capacity

DHS will assemble a cadre of internal and external computational capacity, data storage, and security experts across DHS Components to survey the current state of the Department's AI-ready infrastructure to make recommendations on how it can be improved. DHS Components will then consider the recommendations for their infrastructure investment consistent with Goal Three.

Objective 2.2: Develop Phased Plans to Upgrade Department Infrastructure

Leveraging insights learned through Goal One and its Objectives, DHS will produce a phased plan to upgrade the Department's computational capability, data storage, and associated infrastructure in accordance with the identified risks and needs aligned with related efforts to deploy secure IT systems. The Department will prioritize areas of greatest need from both a technical and risk mitigation perspective.

Objective 2.3: Evaluate and Invest in AI Research and Development

The Department will consistently evaluate AI research and development and invest in technologies with the potential to enhance the homeland security mission.

Objective 2.4: Develop the Department's Budget Requirements for AI

Multiple think-tank, university, and government studies call for a substantial increase to the U.S. Government's overall spending on government AI systems and the funding of research and development to keep the United States in a leadership position in its development. DHS Components will evaluate their current and projected AI needs and produce a projected budget requirement for necessary infrastructure upgrades. Associated resource increases must include both systems and the teams needed to maximize value and provide oversight. Proposed infrastructure upgrades will also improve other mission functions bringing a broad benefit to the Department's capabilities.

Goal Three – Mitigate AI Risks to the Department and to the Homeland

AI will pose evolving risks to DHS activities as we start to incorporate AI systems into our operations. More broadly, AI increased use of AI will also introduce new and evolving risk to the homeland security enterprise as new technologies and applications are relied upon by our partners and stakeholders. This includes risks from adversarial efforts to compromise AI systems or to use AI technology to target the homeland.

Mindful of these risks DHS will produce a comprehensive risk outlook and develop mitigation measures to ensure the continued success of the homeland security mission. DHS will cultivate a robust set of partnerships across the AI and homeland security communities to inform and manage risks related to AI applications.

DHS will also develop the policies, practices, and expertise necessary to serve as a model for AI deployment to organizations that function in complex operating environments. Furthermore, DHS will ensure transparency to the extent practicable around AI determinations that impact individuals or entities so that the American public can understand decision making influenced by AI systems and inform regulatory and policy outcomes.

Objective 3.1: Develop a Process for Continual Evaluation of AI Risks

The pace of research and development of AI technology and applications, as well as the rapid increase in computing power using classical and quantum architectures, demands a constant and continual evaluation of AI risks. Components operating AI systems to support their missions must also continually validate the performance of their system to monitor for and take action to mitigate risks posed by bias or other unintended outcomes. DHS will develop a process by leveraging expertise from inside the Department, private sector, and academia partners to produce a report for the Secretary outlining the current state and projected future risks of AI to the homeland.

Objective 3.2: Produce and Release Public AI Data Use Guidance

The appropriate use of data for the training or operation of an AI system is central to the responsible integration of AI technology into the successful execution of our mission and mitigating certain risks associated with DHS reliance on AI systems. DHS will prioritize the production of specific guidance on the use of data by DHS Components for AI purposes consistent with applicable legal requirements, including requirements related to data use and privacy to avoid issues of efficiency, trustworthiness, and biased system outcomes.

This guidance will, to the extent practicable, be released publicly and will clearly state the circumstances under which different types of data will be used and what measures DHS Components will take to protect privacy and ensure the responsible and trustworthy use of AI by DHS. DHS guidance and strategic vision can serve as a model across the homeland security enterprise for entities using AI systems including our state, local, tribal, and territorial (SLTT) partners, critical infrastructure, and law enforcement consistent with protection of privacy, individual rights, economic development, and national security.

Objective 3.3: Design and Implement a Program to Curate Native Datasets for Optimum AI Use

Human-curated training data for AI systems is critical to ensuring trust in the output and operation of AI systems used by DHS. DHS will ensure that the algorithmic training matches the intended outcome for the system. DHS Components holding data that is currently or may be used in the operation or training of an AI system will design and implement a program to curate their datasets to optimize the use of AI in such a manner that mitigates the potential for biases, which could negatively impact the integrity or reliability of the AI system or degrade public trust, in accordance with the guidance developed by DHS as part of Objective 2.1.

Objective 3.4: Document Smart Engineering and Operating Practices

DHS Components shall include in any proposal for the use of an AI system a mechanism by which the data used to train the system is, to the extent practicable, accessible by managers and operators of the system. The accessibility shall also extend to affected populations outside of certain military, foreign intelligence collection, or law enforcement activities. By doing so, DHS Components will address potential issues with system explainability and operational integrity.

Documentation of engineering and operating practices by DHS Components makes it more feasible to provide assurances of both ethical alignment and operational integrity of AI systems. Components shall also use privacy engineering concepts to the greatest possible extent and document the consideration of these concepts.

The Department will not obscure its use of AI to support operations but will be transparent to the extent practicable, to build public trust and to encourage public and private development of AI systems that are accountable to users, the public, oversight bodies and the legal system. In all cases in which AI is used, operational assessments of potential risk and harm, the magnitude of those risks and harms, the technical state of the art, and the potential benefits of the AI system must be substantiated to facilitate both explainability and transparency.

Objective 3.5: Formalize AI Governance Processes at DHS

DHS will establish a DHS-enterprise wide AI Coordination and Advisory Council (Council) composed of internal subject matter experts to monitor and support the adoption of AI technology by DHS Components. The Council will leverage external and internal experts to assist DHS Components in AI adoption; to study and share best practices from other agencies and the private sector; and to coordinate with internal DHS governance bodies, as appropriate to allow Components to develop unique AI requirements that align with their respective missions. This Council will also consider legal, compliance, classification, civil rights and civil liberties, and privacy implications and responsibilities related to DHS AI projects, methods and capabilities.

Objective 3.6: Targeted Engagement and Education to Homeland Security Enterprise Partners

DHS will prioritize the sharing of risk information associated with the use of AI with SLTT partners, critical infrastructure operators, and other partners in the homeland security enterprise. The Department will also educate these partners on good AI use practices and risk mitigation techniques to ensure the security and responsible use of AI across the enterprise.

Objective 3.7: Community Standards

DHS will support interagency and infrastructure community efforts to institute standards governing responsible use of AI technologies. Through development and communication of shared best practices and standards, infrastructure usage of AI can be more securely deployed.

Objective 3.8: Development of International AI Standards

DHS will seek consistent and ongoing international cooperation from a broad range of partners to focus on the development of mutually agreed upon principles on responsible stewardship of trustworthy AI; multi-stakeholder, consensus-driven global technical standards for interoperability; internationally comparable metrics to measure AI research, development, and deployment.

The increased perspective on AI challenges presented in other countries will allow DHS to anticipate potential risks and respond in an effective manner. Increased cooperation on AI with international partners will also allow the opportunity for the Department to advance the principles of this strategy with like-minded nations.

Objective 3.9: Counter Adversarial Use of AI Against the Department and the Homeland

DHS will take a strategic approach to mitigate and counter efforts by our adversaries to leverage AI technology against the Department and the homeland. DHS will maintain a broad and evolving picture of potential AI risks and AI capabilities of our adversaries to inform the Secretary of potential risks and take effective actions to counter malicious activity.

Goal Four – Develop DHS AI Workforce

Critical to any DHS implementation and maintenance of an AI system is a trained workforce, including AI policy and privacy professionals, that can manage augmentation of current systems with AI functionality, design and implement new AI augmented systems and understand how advances in the field can benefit the Department. DHS Components will prioritize the hiring and development of AI professionals to manage and maintain systems in a manner that preserves public trust in the stewardship of AI systems and associated data. The Department will also engage in outreach to institutions training AI professionals to offer specific internships and fellowships for AI students and professionals. Accomplishment of this goal in the spirit of this strategy will grow and mature an expert cadre of uniquely DHS AI professionals supporting the Department's missions.

Objective 4.1: Identify Current AI Expertise and Gaps Across DHS Enterprise

DHS will evaluate its current AI use footprint and compare its in-house AI experience with the expertise requirements to responsibly manage and operate its systems. DHS will further conduct a survey to identify current employees with AI expertise. These employees will be made available as an enterprise resource on an ad hoc basis for DHS Components lacking sufficient AI experience to evaluate the need for a new AI solution or to evaluate an existing AI system for its overall technical health and for compliance with this strategy, under the oversight of the AI Coordinating and Advisory Council. The gap that exists between the native DHS AI experience and the proliferation of AI use in the Department will inform actions by DHS to recruit and retain AI expertise.

Objective 4.2: Identify External AI Training Courses and Make Available to Workforce

Components will identify external AI training courses consistent with their AI needs and make them available to the workforce. Components should make training funds available to cover the cost of appropriate AI courses. This training program will encourage the growth of an expert AI cadre native to DHS. Along with increased operational effectiveness, AI carries enterprise-level fiscal, legal, security, operational and political risk. Training will, therefore, also be made available to business users, oversight and advisory office staff, managers and leadership who support and have oversight on AI projects. Formal and informal internal training will also be made available, as appropriate.

Objective 4.3: Partner with Academic and Private Sector to Develop a Public/Private Sector Fellowship Program

Consistent with Goal 1, DHS will continue to develop partnerships with academic and private-sector research and technology entities and engage in an exchange program sending DHS employees on rotation to private firms and academic institutions and accepting private and academic researchers and technical experts on rotation to DHS. Fellows will be a key part of future DHS AI workforce and be required to report to their Component and the broader Department on the state of AI research and development and new potential applications impacting Departmental equities. This effort will keep DHS at the leading edge of AI development.

Goal Five – Improve Public Trust and Engagement

The trust of the American people is vital to the success of the implementation and responsible use of AI by the Department. AI technology is not widely understood and, as such, carries a negative connotation with many non-experts. Further, the public must trust that the Department is evaluating AI-enabled threat vectors to the homeland using well-informed experts. Public trust will strengthen the Department's use of AI by ensuring the support of the citizens it intends to protect and guard against reputational impacts to the Department.

DHS will facilitate this trust by engaging strategically with the American public regarding AI. DHS will also ensure that DHS Components fully consider privacy and civil liberty implications when leveraging personal information; engage in a public comment period as appropriate; and consult with the AI Advisory and Coordination Council to ensure Departmental equities are addressed and to leverage expertise from other parts of DHS to support the project. DHS will also seek to engage the public on AI risks to the maximum extent practicable. Accomplishment of this goal will result in an educated and supportive American public who supports the Department's transparent and accountable use of AI in accordance with this strategy and applicable Executive Branch guidance.

Objective 5.1: Develop strategic communications plan to support Communication to the Public on AI

DHS will produce guidance for DHS-wide communication with the public on AI. This communication will apply Department-wide with exceptions for certain military, law enforcement, and intelligence activities and be oriented toward increasing public awareness of AI systems in general and communicating the Department's position on responsible and trustworthy use of human-involved AI with examples of how that position is being carried out.

DHS will also ensure a public communications plan will be developed and implemented across the Department. The communication plan will make clear the importance of AI for protecting the homeland and will also serve to deter adversaries. This plan shall effectively and clearly identify: 1) the intended use, 2) data elements needed for algorithmic training and function, 3) parameters and levels of human oversight and decision making, 4) transparency regarding the collection, use, dissemination, disclosure, and protection of information, 5) benchmarking and subsequent auditing of the system performance, 6) accuracy of results and means of providing individuals redress for inaccuracies, improper use, or disclosure, and 7) decision making parameters performed by humans and by an algorithm.

Objective 5.2: Establish a Framework for Releasing AI System Information for Public Comment

Future AI systems implemented by DHS will require a public release of system information with appropriate exceptions for certain sensitive military and intelligence systems, and some exceptions for law enforcement activities. DHS will produce a framework for releasing AI system information and a process for public comment.

Objective 5.3: Communicate Identified AI-Related Risks

In support of establishing public trust in AI, the Department will seek to communicate the identification of AI-related risks when practical and considering intelligence collection, law enforcement, and military equities.

CONCLUSION

In an age of the reemergence of great power competition, the United States faces threats to its homeland, its citizens, and its values from more vectors than ever before. This fact is compounded by the rapid development of a new technological frontier in AI. AI provides numerous challenges for DHS including its responsible use of AI consistent with American values and securing the homeland in light of new and evolving risks. It is imperative that the Department not only to prevail over these challenges, but also lead in investment and integration of AI technology into accomplishing our mission.

The Department will evolve to ensure it is postured for continued mission success as AI opportunities and risks evolve with the further development of the technology. The Department will act in a way to understand the risks AI poses to its mission and embrace innovation to counter those and other new and emerging risks. The goals and objectives presented in this strategy will therefore position the Department to confront these challenges and to become a leader in the effective adoption, use, and governance of AI and the mitigation of AI-related risks.

The security of our homeland depends on the Department's response to this national imperative. With this strategy, the Department can move forward with concrete and tangible goals to answer the challenges and create a safer homeland while preserving American values.