S&T ARTIFICIAL INTELLIGENCE & MACHINE LEARNING STRATEGIC PLAN

Homeland
Security
Science and Technology

AUGUST 2021

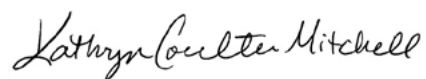# LETTER FROM SCIENCE & TECHNOLOGY LEADERSHIP

Science and technology innovations help our nation answer the threats of tomorrow and the needs of today. Leading research and development for the homeland security mission, the U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T) has the power to bring the right partners together to solve mission-critical problems for the Department's frontline employees as they protect and secure our nation. By leveraging current and emerging scientific advancements, S&T supports immediate DHS Component operational gaps while preparing the Department to address future threats.

Artificial Intelligence is a revolutionary capability that presents substantial opportunities for DHS to more efficiently and effectively accomplish our mission to secure the homeland. Effective implementation will also require significant expertise, coordinated research and development, and targeted investments.

I am proud to introduce the S&T Artificial Intelligence/Machine Learning Strategic Plan, which lays out an actionable path for S&T to advise and assist the Department in harnessing the opportunities of Artificial Intelligence and Machine Learning (AI/ML). Through this strategy, S&T will build and apply expertise to help the Department fulfil the game-changing promise of AI/ML technologies while mitigating the inherent risks.

As we grow S&T's proficiencies in artificial intelligence and machine learning, we ensure S&T continues supporting the Department's vision to enhance its capability to safeguard the American people, our homeland, and our values through the responsible integration of artificial intelligence into the Department's activities.

Sincerely,

Kathryn Coulter Mitchell

Kathryn Coulter Mitchell

Senior Official Performing the Duties of Under Secretary for Science and Technology

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

The U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T) presents goals that will enable S&T to conduct Artificial Intelligence and Machine Learning (AI/ML) research, development, test, and evaluation activities to support DHS mission needs, and to advise stakeholders on developments in AI/ML and the associated opportunities and risks.

The S&T AI/ML Strategic Plan defines S&T's approach to effectively address the opportunities and challenges that AI/ML poses to the Department, the broader Homeland Security Enterprise, and the missions they serve. The S&T AI/ML Strategic Plan presents three goals:

GOAL 1: *Drive Next-Generation AI/ML Technologies for Cross-Cutting Homeland Security Capabilities*

S&T will make strategic investments in AI/ML research and development activities that meet critical DHS needs. S&T has identified three R&D objectives: Advance Trustworthy AI, Advance Human Machine Teaming, and Leverage AI/ML for Secure Cyberinfrastructure. Advancing Trustworthy AI is an interdisciplinary effort to research and provide actionable solutions for issues such as explainable AI, privacy protection, countering bias, and countering adversarial machine learning. S&T will research Human Machine Teaming, optimizing human and machine interactions while limiting their weaknesses. In the area of Secure Cyberinfrastructure, S&T will research capabilities that allow data sharing and processing across systems, effective management of AI/ML models, and AI/ML capabilities that enable threat detection and response.

GOAL 2: *Facilitate Use of Proven AI/ML Capabilities in Homeland Security Missions*

S&T will identify technically mature capabilities and match them to mission needs to facilitate understanding and adoption of existing AI/ML solutions by DHS Components and stakeholders. S&T will also advance capabilities that can be used by non specialists to curate and process large datasets, while advising the Department on the technical and policy infrastructure needed for AI/ML.

GOAL 3: *Build an Interdisciplinary AI/ML-Trained Workforce*

S&T will recruit experts and train current personnel to improve AI/ML competence across the S&T workforce in order to more effectively achieve S&T missions. Additionally, S&T will provide expert advice and recommendations for training opportunities to the broader DHS and Homeland Security Enterprise (HSE)[i] communities.

S&T's approach to AI/ML is informed by national guidance and the **DHS Artificial Intelligence Strategy**. S&T leadership is committed to ensuring that AI/ML research, development, test, evaluation, and departmental applications comply with statutory and other legal requirements, and sustain privacy protections and civil rights and civil liberties for individuals. A subsequent S&T AI/ML Implementation Plan will detail how the S&T AI/ML Strategic Plan will be operationalized.

II. PURPOSE

The S&T Artificial Intelligence and Machine Learning Strategic Plan establishes the S&T AI/ML vision, mission, goals, and objectives. The Strategic Plan identifies the focus areas for AI/ML that S&T will address to carry out its missions as the research and development arm and science and technology advisor to DHS Components, DHS Headquarters, and the Homeland Security Enterprise.

III. INTRODUCTION

A. AI/ML in DHS Mission Context

DHS missions include, for example, managing cyber and physical risks to critical infrastructure, securing American borders while facilitating lawful trade and travel, preventing and investigating criminal activity, and responding to natural and human-made disasters. AI/ML presents opportunities to more efficiently and effectively accomplish the many and varied missions of the DHS Components and the broader HSE. Examples of possible uses for AI/ML in these missions include processing large quantities of sensor data at border crossings, scanning cyber activity for anomalies, and modeling the effects of a natural disaster on critical infrastructure. AI/ML also introduces new risks, which DHS must be prepared to identify, assess, and mitigate. DHS must develop and field this new technology in a way that protects privacy, civil rights and civil liberties, and protects against bias, both to ensure effectiveness and to maintain public trust. DHS must also be prepared to respond effectively to issues when they occur.

B. AI/ML in S&T Mission Context

S&T's mission is to safeguard the nation by answering the threats of tomorrow and the needs of today through science, technology, and innovation. Created by the Homeland Security Act of 2002, S&T conducts basic and applied research, development, demonstration, testing, and evaluation activities relevant to DHS and the HSE. The S&T AI/ML Strategic Plan meshes with and is supported by the goals articulated in the 2021 S&T Strategic Plan. As the research and development arm of DHS and trusted science and technology advisor to DHS Components and HSE stakeholders, S&T will conduct research to understand opportunities and risks associated with rapidly changing AI/ML technologies and impacts to DHS missions.

S&T will enable DHS and the broader HSE to effectively use AI/ML to carry out their missions of protecting the American people and the homeland, while operating with ethical standards and in accordance with the values of the American people. S&T leadership is committed to ensuring that AI/ML research, development, test, evaluation, and departmental applications comply with statutory and other legal requirements, sustain privacy protections, and maintain civil rights and civil liberties for individuals.

C. S&T AI/ML Vision

S&T is the Department's trusted advisor for AI/ML, providing expert, independent, and objective technical guidance for research, acquisition, and implementation of AI/ML capabilities for critical homeland security missions in partnership with federal, industry, academia, and international partners. S&T anticipates how the increasing ubiquity of AI/ML in society, including the use of AI/ML by adversaries, may impact DHS and the HSE. Additionally, S&T informs and fosters DHS Components' assessment and potential acquisition of AI/ML capabilities. Finally, S&T possesses organizational capacity to understand the opportunities and risks in the rapidly changing field of AI/ML, in order to advance DHS missions.

D. Definitions of AI/ML

Artificial Intelligence

"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" (DHS Artificial Intelligence Strategy, December 3, 2020).

Machine Learning

Machine Learning (ML) is a subset of AI. ML systems receive inputs in the form of training data, and then generate rules that produce outputs. In other words, ML systems "learn" from examples, provided in the form of training data, rather than receiving explicit programming from humans. In recent years, increasing availability of very large datasets, developments in available computing power, and other technical advances have made ML useful and promising for a variety of applications.

As AI/ML technologies advance, DHS must continually assess the opportunities and risks associated with their uses in order to ensure that DHS can effectively leverage emerging technologies to achieve its missions, while anticipating new dependencies associated with algorithmic decision-making. DHS will ensure that the use of AI/ML meets ethical standards and promotes and protects U.S. interests. S&T will advise DHS Components and partners on state-of-the-practice to effectively prevent, deter, or counter threats.

E. Strategy Development Process

The S&T AI/ML Strategy Working Group, led by the Technology Centers Division and including a matrixed membership from across S&T, convened in Summer 2020 to identify and scope core areas of research and development activity that will serve to inform, educate, and improve S&T's program areas as well as the Department's activities impacted by this disruptive technology. Its assessments were informed by national guidance, DHS policy, and DHS Component outreach to coordinate and focus current and future activities in AI/ML within S&T.

The goals and objectives below were informed by a series of workshops held in October and November 2020 with operators, program managers, technologists, senior leaders, and decision-makers from across DHS. S&T's goals align with those outlined in the DHS AI Strategy and specify S&T's research and development priorities in AI/ML.

IV. VALUES AND PRINCIPLES

The S&T AI/ML Strategic Plan aligns with the department-wide DHS Artificial Intelligence Strategy (December 3, 2020) and overarching DHS Guiding Principles by specifying how S&T will support and address the research and development challenges and opportunities that emerging AI/ML technologies pose to the Department. S&T is guided by the principles set forth in Executive Order 13859 "Maintaining American Leadership in Artificial Intelligence" (February 11, 2019) and Executive Order 13960 "Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government" (December 3, 2020), as well as the National Institute of Science and Technology report U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools (August 9, 2019). Further, S&T acts in accordance with the AI principles advanced by Organization for Economic Cooperation and Development (OECD) member countries and adopted by the G20.

These principles will inform the development of a subsequent S&T AI/ML Implementation Plan that describes a roadmap and governance approach for achieving the goals, objectives, and outcomes outlined in this S&T AI/ML Strategic Plan.

V. GOALS

The DHS AI Strategy (December 3, 2020) sets out five goals to govern the Department's approach to integrating AI into the DHS mission in a responsible and trustworthy manner and successfully mitigating risks associated with AI across the HSE. The DHS AI goals are:

DHS AI GOALS

1	2	3	4	5
ASSESS POTENTIAL OF AI ON THE HOMELAND SECURITY ENTERPRISE	INVEST IN DHS AI CAPABILITIES	MITIGATE AI RISKS TO THE DEPARTMENT AND TO THE HOMELAND	DEVELOP A DHS AI WORKFORCE	IMPROVE PUBLIC TRUST AND ENGAGEMENT

In addition to aligning with efforts across DHS and the HSE, S&T will continue to engage interagency, academic, industry, and international partners to offer evidence-based guidance for HSE mission and support challenges. S&T establishes three strategic goals to advance the organization's role in AI/ML at DHS:

— S&T AI/ML GOALS —

1
DRIVE
NEXT-GENERATION AI/ML TECHNOLOGIES FOR CROSS-CUTTING HOMELAND SECURITY CAPABILITIES

2
FACILITATE
USE OF PROVEN AI/ML CAPABILITIES IN HOMELAND SECURITY MISSIONS

3
BUILD
AN INTERDISCIPLINARY AI/ML TRAINED WORKFORCE

Goal 1: Drive Next-Generation AI/ML Technologies for Cross-Cutting Homeland Security Capabilities

S&T partners with academia, industry, international and federal, state, and local partners to make research investments that leverage AI/ML breakthroughs for Homeland Security needs. S&T Strategic Goal One aligns with DHS AI Strategy Goal Two: *Invest in DHS AI Capabilities*. The priority areas for S&T's investments in AI/ML are Advancing Trustworthy AI, Human-Machine Teaming, and Secure Cyberinfrastructure. These priority areas were formulated and validated by the S&T AI/ML Working Group, based on alignment with existing and projected S&T and Component needs.

Objective 1A: Advance Trustworthy AI

Advancing Trustworthy AI is a broad research area examining how to ensure confidence in AI/ML systems. This research area is critical for DHS and the HSE for multiple reasons:

- To enable DHS leaders and managers to effectively assess the performance of AI/ML systems against both technical and mission metrics, as well as meeting applicable legal and policy requirements;

- To provide operators making critical decisions an appropriate level of trust and confidence in any AI/ML systems incorporated into their mission; and

- To inspire trust in the general public towards AI/ML systems deployed by DHS.

- The problems addressed in this area of research are not only technical, but are truly multi-faceted and require the full spectrum of the social sciences, as well as policy, legal, privacy, civil rights and civil liberties, and ethics research to develop governance approaches that build trust within DHS, the HSE, and broader society. There is considerable overlap among the critical areas included in Advancing Trustworthy AI.

1A.i Advance Explainable AI: S&T will support research in Explainable AI, through investments, collaborations, and knowledge-sharing, in order to promote research advances that would make responsible and trustworthy implementation of AI in DHS and HSE contexts possible and to facilitate legal and administrative processes for individuals who are affected by DHS activities that rely on AI/ML tools. Effective use of AI/ML requires explanations for how the systems work that are understandable and meaningful to DHS stakeholders, including oversight stakeholders. This requires technical research into how to effectively audit an AI/ML system to understand how it arrived at its outputs. Research into how humans understand and interpret the explanations is also necessary. This includes ensuring that the technical audit incorporates social, behavioral, and ethical considerations as well as legal, policy, and privacy requirements of DHS and HSE operations and that explanations are useful and meaningful to DHS and HSE personnel.

1A.ii Build Privacy Protections within AI Capabilities: Many AI/ML models are trained on and process vast amounts of data. Research on new approaches to privacy protections can benefit DHS by ensuring that the data is collected, used, maintained, and disseminated in a manner that adheres to privacy laws, regulations, and DHS policies, while maintaining public trust. S&T research will include how policies, business rules, and innovative

privacy enhancements can best ensure privacy for AI/ML capabilities. S&T will also research new and innovative privacy enhancements and protections, and how to train AI/ML models to process data in ways protect individuals' privacy. This research will inform guidance that S&T provides to Components.

1A.iii Advance the Ability to Detect and Counter Bias in AI/ML Capabilities: AI/ML models are trained on datasets that may possess or introduce forms of bias that can then be replicated or amplified by machine processes. This may include treating individuals in a manner inconsistent with Constitutional and legal guarantees of equality, or in some cases magnifying or exacerbating systemic social biases and creating disparate impacts. This could result in impermissible or adverse consequences for these groups, which is in fundamental contradiction to the core values and missions of DHS and the HSE: to protect the American people and uphold their values. Understanding how impermissible biases occur and detecting them prior to incorporation in an AI/ML solution is therefore a critical avenue of interdisciplinary research that S&T will undertake.

1A.iv Ensure Trust in AI/ML Capabilities: This area aligns with DHS AI Strategy Goal Five: *Improve Public Trust and Engagement.* It is important for those who interact with or are affected by AI/ML systems to have an appropriate level of trust. If the general public lacks confidence in AI/ML used by DHS and the HSE, then its use may undermine public trust and become a barrier to DHS and its Components performing its missions. S&T will pursue interdisciplinary research to assess how the public perceives AI/ML in homeland security applications and what methods and approaches will best build public trust. S&T believes such research can help to ensure that DHS and the HSE develops and uses AI/ML in ways that are in accord with community values and interests. Additionally, S&T will identify and leverage best practices—including those of industry—to ensure that potential implementations of AI/ML meet technical and ethical standards. If DHS does not incorporate technically and ethically sound technologies into its mission as industry and adversaries advance, DHS Component and HSE effectiveness may decline, which would negatively impact public perception.

1A.v Counter Adversarial Uses of Machine Learning[ii]: While AI/ML can bring enormous benefits, it also creates unique vectors of attack. An AI/ML model's universe is rooted in its training data. If that data is compromised, AI/ML systems can be trained in ways that result in negative outcomes. Alternately, adversaries can identify limitations in training data and take advantage of them. Additionally, the AI/ML model can also be attacked, stolen, spoofed, or modified. Research to understand, prevent, and counter adversarial machine learning is essential for developing trustworthy AI for DHS and the HSE.

Objective 1B: Advance Human-Machine Teaming

This objective is to conduct research into how humans and AI/ML can collaborate most effectively to carry out the missions of DHS and the HSE. AI/ML has very specific strengths and weaknesses – as do human beings. Understanding how AI/ML can most effectively augment human decision-making is critical to maximizing the potential benefits of AI/ML to DHS and the HSE. This area of research is interdisciplinary and requires the blending of technical research with social science.

1B.i Optimize Human-in-the-Loop Architecture: Given the sensitivity of DHS Component and HSE operations and the brittleness[iii] of AI/ML, constructing systems that fully engage human capabilities in order to get the best of both human cognition and computational processing is a critical priority. S&T will build on the extensive research in this area to develop solutions that will meet DHS mission needs.

1B.ii Enable Collaboration Between Users and Heterogenous Architecture: The explosive growth in sensors, processing, and data throughout society, particularly with the emergence of Internet of Things (IoT) and edge computing, creates new opportunities for DHS Components and the HSE to use data in an array of crisis and commonplace situations. This data, however, exists and will exist in varied architectures. S&T will conduct research into developing AI/ML that can – in real time – operate across varied architectures in order to leverage this data.

Objective 1C: Leverage AI/ML for Secure Cyberinfrastructure

Cyberinfrastructure "consists of computing systems, data storage systems, advanced instruments and data repositories, visualization environments, and people, all linked together by software and high performance networks to improve research productivity and enable breakthroughs not otherwise possible."[iv] Cyberinfrastructure undergirds critical infrastructure sectors, the security of which is a mission of DHS. The technological revolution that enables cyberinfrastructure also underpins AI/ML. Given the speed, scale, and computationally intensive demands of cyberinfrastructure, AI/ML is an essential tool in its security.

1C.i Characterize Effective Model Lifetimes: S&T will research the efficacy of AI/ML models, including how best to keep them up-to-date, in order to make recommendations and inform stakeholders on how to effectively manage AI/ML across the lifecycle.

1C.ii Enable Rapid Threat Detection and Response: Given the speed at which cyber threats can emerge, propagate, and evolve, strict reliance on human cognition is inadequate to process them in real-time. S&T will research, develop, test, and evaluate AI/ML capabilities that can identify and track emerging cyber threats in real time.

1C.iii Enable Real-Time and Secure Shared Computations: Much of the data and many of the systems critical to analyzing cyber threats and securing cyberinfrastructure have sensitivities such as security classification, PII, or proprietary information. S&T will research technical capabilities that allow sharing and processing of data across systems, while ensuring authorized access and use and not exposing sensitive information.

Goal 1: Outcomes

Some specific outcomes that will indicate progress in meeting DHS needs include:

- **Effective Model Performance:** Effective model performance relies upon well curated data sets. In most cases, S&T will endeavor to use real operational data to train AI/ML models, and to validate and verify model performance. For certain specific homeland security missions, however, collecting sufficient data to train an AI/ML model is not feasible. For these limited cases, achieving several of the objectives will require accurate, reliable models trained on synthetic data. Developing, testing, and evaluating models built with well-curated datasets will drive next-generational AI/ML technologies.

- **Security Mechanisms that Mitigate Reverse Engineering:** Understanding, preventing, and countering adversarial machine learning requires research to characterize threats and vulnerabilities in AI/ML systems. Security mechanisms that reduce risks will be a key indicator in countering adversarial machine learning. This outcome aligns with DHS AI Strategy Goal Three: Mitigating AI risks to the Department and the Homeland.

- **Human Focus Shifts to Cognitively Engaging Tasks:** One promise of AI/ML is to free humans from rote tasks in order to enable them to focus on more complex tasks that rely on human judgment. Properly implemented, AI/ML holds the potential to augment human intelligence in a variety of contexts in which well-characterized, rote tasks are currently executed by human analysts and operators. Developing performance metrics for human-machine teaming in particular DHS applications is an outcome that will enable effective development, testing, and evaluation.

- **Effective Metrics for Understanding Risk in Automated Systems:** Whether ascertaining the privacy risks of an AI/ML system or its potential for error in detecting threats, systematic measures of these risks are needed to determine if the system is meeting its requirements.

Goal 2: Facilitate Use of Proven AI/ML Capabilities in Homeland Security Missions

This goal supports DHS AI Strategy Goal One: Assess Potential Impact of AI on the Homeland Security Enterprise and DHS AI Strategy Goal Two: Invest in DHS AI Capabilities. S&T enables DHS Components and HSE partners to assess and potentially adopt AI/ML in the near-term. S&T will work with Components to understand Component needs, and then will tailor AI/ML research to those needs. S&T's role includes identifying current technologies that can support HSE missions, supporting the Components in building the capacity to adopt AI/ML, developing test and security standards, and advising the HSE of the mission impacts of malicious or disruptive uses of AI/ML.

Objective 2A: Identify, Evaluate, and Transition Existing AI/ML Capabilities for DHS Component and HSE Missions

2A.i Develop or Adopt Proven AI/ML Capabilities to Meet Component Needs: In coordination with Components, S&T will work to understand Component needs and capabilities, and the policy and mission contexts within which an AI/ML system would operate, in order to tailor S&T research and development to fill capability needs.

2A.ii Identify, Evaluate, and Transition Capabilities and Inform Stakeholders: If mature AI/ML capabilities exist, DHS must be in a position to evaluate their technical performance and potential mission impacts. This process includes matching the right technology to the appropriate mission, given the analytical maturity of the Component or partner and of their operators. This process is not only technical. Enabling the DHS Components and HSE to adopt AI/ML will need to draw upon the full spectrum of capabilities at S&T including social science, systems engineering, test and evaluation, human factors, and organizational analysis. Even if a capability is technically robust, determining if it fits the context of use, end-user requirements, and other strategic and tactical considerations is a process that necessitates the participation and judgment of diverse subject matter expertise.

2A.iii Conduct Pilot Studies: S&T will conduct pilot studies on promising technologies in order to rapidly experiment with AI/ML systems that may provide value to DHS Components. Such pilot studies will enable S&T to inform stakeholders about the functionalities of existing capabilities, and to potentially transition viable products to serve DHS Components' mission needs.

Objective 2B: Enable AI/ML throughout DHS Components and the HSE

S&T aims to enable innovation at every level of the HSE by identifying, evaluating, and advising on tools and capabilities that will enable Components and partners to better understand how AI/ML solutions can address mission challenges. This objective calls for a spectrum of technical investments while supporting Components in their organizational learning.

2B.i Guide Components on Accessible AI/ML Tools: As AI/ML advances, tools that enable its use by non-data scientists are becoming commercially available. These tools facilitate implementing AI/ML solutions in DHS and the HSE. S&T will provide guidance to Components on these capabilities, including self-service, data cleaning and prep capabilities, and accessible AI/ML tools. S&T will also inform stakeholders on potential governance issues associated with accessible AI/ML tools.

2B.ii Advise Components on Technical AI Architecture Investments: S&T will serve as advisor to Components making investments into architecture that enables AI to ensure that Components' needs will be met in the most effective manner possible and to ensure that architecture choices at the component level do not hinder data sharing at the enterprise level.

2B.iii Serve on DHS AI Governance Body: Enabling the success of technology adoption by organizations requires effective governance. The DHS AI Strategy mandates the formation of a governance body at DHS. S&T will be represented on this governance body and will serve a critical role by providing science and technology guidance. Governance in this context may be informed by or help to inform areas such as: policy, ethical standards, data curations, resource allocation, protecting privacy, civil rights and civil liberties, records management, and acquisition regulations, and providing Department and senior leadership the tools they need to manage both the enterprise-level risks and benefits of AI adoption. S&T will also provide technical advice on AI/ML to support partners and Components in developing their own governance structures, in order to properly implement AI/ML in the DHS Components and HSE.

2B.iv Guide Components on Automated Data Governance: Accessing and using datasets often entails an extensive process of approvals. Automated data governance tools and capabilities, available commercially or being developed, could accelerate this process while ensuring that policy and records management requirements are met. S&T will experiment with and provide guidance on automated data governance capabilities and opportunities. Automated data governance tools can speed information access, sharing, and processing and, at the same time, better secure adherence to standards of privacy, civil rights and civil liberties, and other legal and policy requirements.

2B.v Advise and Determine Countermeasures for Malicious AI Use: S&T will provide advice to stakeholders about the implications of AI/ML. Malicious use of AI/ML as well as increased AI/ML presence throughout society will have implications for DHS Components' and HSE missions. S&T expertise in AI/ML can help Components and partners develop appropriate proactive measures and responses.

Goal 2: Outcomes

Accelerating state-of-the-art AI/ML capabilities for critical homeland security missions means facilitating DHS Component and stakeholder adoption of proven AI/ML solutions. There are several outputs associated with this goal, including:

- **Technology Assessments Against Critical Missions and Operations:** S&T will provide expert inputs for regular analyses and assessments of the utility of existing technologies to meet mission critical needs.

- **Impacts on DHS Business Processes:** S&T will provide guidance on the potential implications for introducing AI/ML into existing S&T workflows and business processes, as well as for establishing new workflows and business processes that leverage AI/ML. S&T will contribute technical expertise to broader DHS assessments of potential impacts of AI/ML on enterprise business processes.

- **Joint Experiments with Components:** Close collaboration between S&T and Components to run experiments and identify solutions that support the mission will ensure that appropriate technical, organizational, and other considerations are brought to bear when introducing innovations.

- **Well-Informed AI/ML Investments Across DHS:** S&T will generate knowledge products that inform the Components about the latest AI/ML tools, technologies, skills and techniques. Knowledge products will enable the Components to make well-informed investments in AI/ML. This outcome will also support DHS AI Strategy Objective 1.1: Develop Knowledge of Technical Applications of AI and DHS S&T AI/ML Strategy Objective 3B: Enabling Broader DHS AI/ML Competence.

- **Components use S&T Acquisition Guidance:** S&T will provide support to program offices throughout the acquisition process with regard to requirements development, analytic processes, use of standards, systems engineering, and technology readiness, and specific, actionable advice about AI/ML systems that can best meet Components' needs.

- **Engage Partners Via a Community of Practice:** For AI/ML to be adopted across DHS, S&T will need to be embedded in a Department-wide network of AI/ML experts and users who are in regular communication and sharing best practices and insights. S&T will also be represented on the GSA government-wide AI community of practice.

- **Outreach and Communications Guidance:** Building public trust in AI/ML, establishing appropriate use, and other effectively communicating with stakeholders are integral to using this technology in the Homeland Security domain. S&T, in conjunction with other headquarters elements, will play a central role in providing guidance to the Department on these outreach and communications issues.

Goal 3: Build an Interdisciplinary AI/ML-Trained Workforce

Adopting AI/ML requires a workforce familiar and comfortable with the technology. To conduct AI/ML research and advise DHS and the HSE on AI/ML, S&T will lead the way by building a cadre of AI/ML experts with an array of disciplinary backgrounds and perspectives, including system architects, data scientists, engineers, computer scientists, social scientists, privacy professionals, ethicists, and policy analysts. S&T will also work to support DHS and the HSE as they build their own AI/ML enabled workforces. This goal aligns with DHS AI Strategy Goal Four: Develop DHS AI Workforce, as well as the S&T Strategic Plan 2021 goal to advance the S&T workforce to prepare for the future while safeguarding today. S&T will provide and communicate training opportunities in AI/ML, and will play a role in training the broader DHS workforce to promote better understanding about the opportunities and challenges of using AI/ML in DHS missions.

Objective 3A: Build AI/ML S&T Workforce

S&T will train and develop an interdisciplinary workforce, augmenting the expertise of the federal workforce with contractors, FFRDCs, national laboratories, Centers of Excellence, interns, and fellows. This requires more strategic recruitment of AI/ML talent as well as systematic efforts to retain and grow talent in order to build institutional knowledge.

3A.i Recruit: Given the competitive marketplace for AI/ML talent, S&T will work to establish and stabilize a pipeline for AI/ML talent to meet S&T and support DHS needs. One mechanism for building this pipeline is expanding DHS Fellowship programs that promote the development of AI/ML talent by offering faculty, post-docs, graduate students, and undergraduate students direct exposure to unique homeland security challenges. Use of the STEM (Scientific, Technical, Engineering, and Mathematics) hiring authority is another important recruitment avenue. Recruitment and hiring will be facilitated by integrating AI/ML competencies into an already established and approved job series identified by the Office of Personnel Management (OPM).

3A.ii Retain: S&T will improve how it communicates and delivers the value proposition of government service. S&T will explore hiring options, including offering competitive salary and opportunities and applying existing specialized DHS retention incentive plans and bonuses in order to recruit AI/ML talent. To retain talented AI/ML personnel, S&T must ensure that technical capabilities and policy frameworks are in place to allow talented experts to contribute to AI/ML research and development activities.

3A.iii Develop: S&T will create opportunities for highly skilled employees to develop professionally, including career path development that provides for AI/ML experts to seek new challenges within S&T, undertake details with other agencies, and participate in externships that enable the S&T workforce to keep abreast of AI/ML developments in industry, academia, and the non-profit sector.

3A.iv Improve AI/ML Competence Across S&T Workforce: S&T will provide training opportunities to its workforce to quickly impart some technical proficiency in AI/ML for all levels of familiarity.

Objective 3B: Enable Broader DHS AI/ML Competence

For AI/ML to be broadly adopted across the HSE, the workforce must have the skills and knowledge to interact with the technology and to have informed discussions with internal and external stakeholders about it. S&T will play a central role in enabling the broader DHS workforce to understand and make use of AI/ML to fulfill their missions while adhering ethical standards and the principles of Executive Order 13960. S&T will do this by identifying and undertaking training activities and by developing criteria to evaluate technical expertise, in conjunction with DHS Office of the Chief Human Capital Officer (OCHCO) and Office of Personnel Management (OPM).

3B.i Train the DHS Workforce: Across the board, from executives leading agencies to frontline operators, and the array of personnel needed to support them, the DHS workforce needs familiarity with AI/ML. Given a baseline level of knowledge, those inclined will be able to innovate and see new opportunities to use AI/ML for their mission. S&T, as it undertakes its own culture shift, will carry out training and will identify AI/ML training that will enable the DHS workforce.

3B.ii Support DHS Components in Evaluating Technical Expertise of Hires: Just as S&T will need to expand its cadre of AI/ML professionals, Components will need their own cadre of professionals. Determining if a potential hire has the right technical skills for a position is crucial for ensuring that critical positions are properly staffed. S&T, leveraging its contacts in industry and academia, can support Components in evaluating technical expertise of candidates. New processes can be developed to assess, align, and improve the technical health of the Department. S&T, in conjunction with DHS OCHCO and OPM, will support the development of criteria for evaluating technical expertise.

Goal 3: Outcomes

A key outcome of S&T efforts to build an interdisciplinary AI/ML-trained workforce is attracting, developing, and retaining talented AI/ML professionals. There are several other outcomes linked to building an AI/ML workforce, including those that pertain to human resources, training, and fulfillment of S&T's role as trusted science and technology advisor:

- **Provide S&T Expertise Department-wide:** Providing expert advice to DHS Components regarding AI/ML will indicate that S&T is fulfilling its role within the Department, and maintaining a strong positive reputation for providing technical and scientific advice. One important outcome will be that S&T continues to field requests for support from Components on AI/ML problems.

- **Hire Experts:** Hiring experts will ensure that S&T can continue to perform its vital mission of advising the Department.

- **Execute Externships:** Keeping abreast of developments in the rapidly changing AI/ML domain will require S&T experts to regularly spend time in academia and industry. An AI/ML externship program will enable S&T to facilitate these exchanges.

- **Host Interns:** S&T will continue to host interns with engineering, computer science, data science, artificial intelligence, and machine learning backgrounds. Internship programs are a pipeline for bringing AI/ML talent to S&T.

- **Offer Post-Internship Opportunities:** Developing opportunities for interns to remain engaged with homeland security topics will extend the talent pipeline by encouraging AI/ML professionals to continue to contribute to public service.
- **Offer S&T AI/ML Training and Enrichment Opportunities:** S&T will continue to offer seminars and training on the full spectrum of AI/ML applications and issues (including technical, policy, ethical, and societal dimensions) for all levels of knowledge and experience.

VI. CONCLUSION

The S&T AI/ML Strategic Plan presents the vision, goals, objectives, and outcomes that constitute the S&T approach to the emerging opportunities and risks of AI/ML. For complex and rapidly evolving technologies such as AI/ML, building a robust portfolio of research and development activities and an interdisciplinary AI/ML-trained workforce in support of the DHS mission is essential. A subsequent S&T AI/ML Implementation Plan will detail how the S&T AI/ML Strategic Plan will be operationalized.
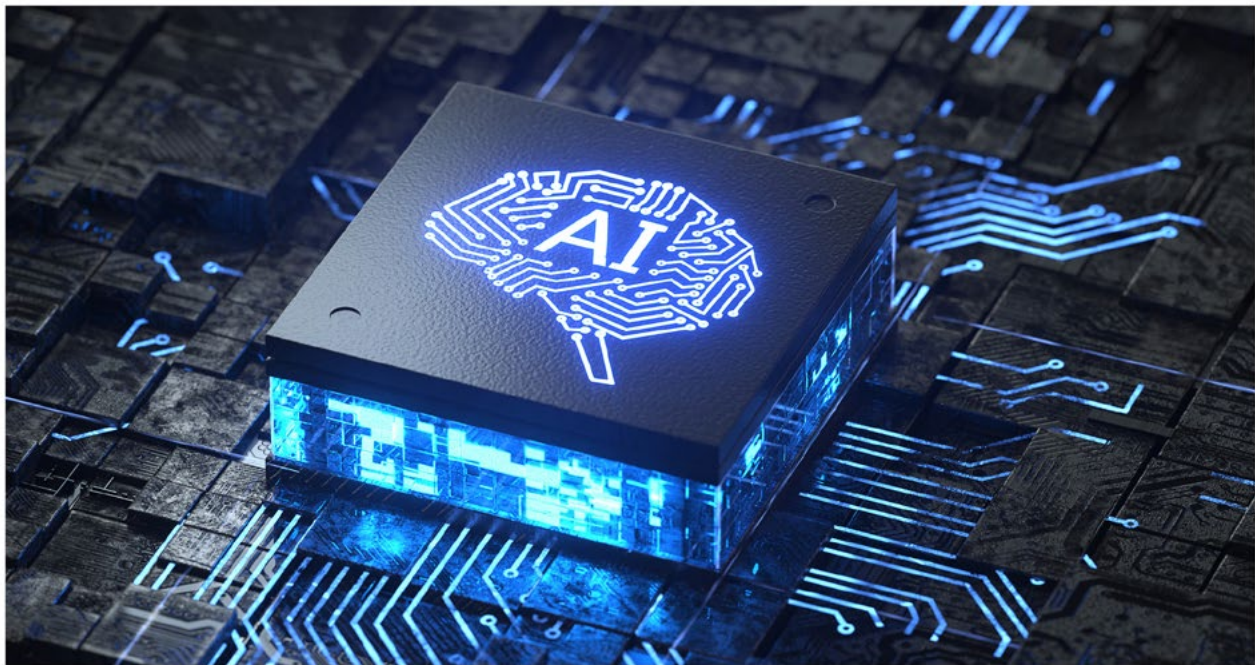
VII. APPENDICES

A. Acronyms

AI – Artificial Intelligence

AI/ML – Artificial Intelligence and Machine Learning

DHS – U.S. Department of Homeland Security

FFRDC – Federally Funded Research and Development Centers

GSA – General Services Administration

HSE – Homeland Security Enterprise

IoT – Internet of Things

ML – Machine Learning

OCHCO – DHS Office of the Chief Human Capital Officer

OPM – Office of Personnel Management

PII – Personally Identifiable Information

R&D – Research & Development

S&T – DHS Science and Technology Directorate

STEM – Science, Technology, Engineering, and Mathematics

U.S. – United States of America

B. References

Allen, Greg, Chief of Strategy and Communications, Joint Artificial Intelligence Center (JAIC), Department of Defense. (April 2020) "Understanding AI Technology: A concise, practical, and readable overview of Artificial Intelligence and Machine Learning technology designed for non-technical managers, officers, and executives". https://www.ai.mil/docs/Understanding%20AI%20Technology.pdf

Department of Homeland Security, Guiding Principles
https://www.dhs.gov/guiding-principles

Department of Homeland Security, Quadrennial Homeland Security Report, January 2010
https://www.dhs.gov/xlibrary/assets/qhsr_report.pdf

Department of Homeland Security Artificial Intelligence Strategy (December 3, 2020)
https://www.dhs.gov/sites/default/files/publications/dhs_ai_strategy.pdf

Department of Homeland Security S&T Strategic Plan 2021
https://www.dhs.gov/sites/default/files/publications/21_0121_st_strategic_plan_2021_final.pdf

Executive Order, "Maintaining American Leadership in Artificial Intelligence" (EO 13859, Feb 11, 2019)
https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence

Executive Order, "Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government" (EO 13960, Dec 3, 2020)
https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government

NIST, U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools (August 9, 2019)
https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf

ODNI, Principles of Artificial Intelligence Ethics for the Intelligence Community
https://admin.govexec.com/media/principles_of_ai_ethics_for_the_intelligence_community_(1).pdf

ODNI, Artificial Intelligence Ethics Framework for the Intelligence Community. June 2020
https://admin.govexec.com/media/ai_ethics_framework_for_the_intelligence_community_1.0.pdf

ODNI, The AIM Initiative: A Strategy for Augmenting Intelligence Using Machines. 2019.
https://www.dni.gov/files/ODNI/documents/AIM-Strategy.pdf

OECD Principles on AI
http://www.oecd.org/going-digital/ai/principles/

OSTP, Artificial Intelligence for the American People
https://trumpwhitehouse.archives.gov/ai/

Stewart, Craig A., Stephen Simms, Beth Plale, Matthew Link, David Y. Hancock, and Geoffrey C. Fox. "What is cyberinfrastructure?" In Proceedings of the 38th annual ACM SIGUCCS fall conference: navigation and discovery, pp. 37-44. 2010.
http://dsc.soic.indiana.edu/publications/fp109a-stewart.pdf

C. Endnotes

[i]"The "Homeland Security Enterprise" refers to the collective efforts and shared responsibilities of Federal, State, local, tribal, territorial, nongovernmental, and private-sector partners as well as individuals, families, and communities—to maintain critical homeland security capabilities." (Department of Homeland Security, Quadrennial Homeland Security Report, January 2010, pp. 12-13)

[ii]Adversarial Machine Learning refers to the range of techniques that can be used to manipulate an AI/ML model.

[iii]In the context of AI/ML systems, "brittleness" refers to the inability of algorithms to function well beyond the set of originally-defined conditions or parameters in which they were developed. AI/ML systems that effectively solve a problem under narrow constraints may not generalize or apply to other contexts.

[iv]Stewart, Craig A., Stephen Simms, Beth Plale, Matthew Link, David Y. Hancock, and Geoffrey C. Fox. "What is cyberinfrastructure?" In Proceedings of the 38th annual ACM SIGUCCS fall conference: navigation and discovery, pp. 37-44. 2010.

ONLINE
www.dhs.gov/cyber-research

EMAIL
SandT-Cyber-Liaison@hq.dhs.gov

TWITTER
@dhsscitech

LINKEDIN
www.linkedin.com/company/dhsscitech

FACEBOOK
Facebook.com/dhsscitech

YOUTUBE
www.youtube.com/dhsscitech

PERISCOPE
@dhsscitech