TESTIMONY OF
W. Douglas Maughan, Ph.D.
Division Director, Cyber Security Division
Science & Technology Directorate
U.S. Department of Homeland Security
Before the
House Committee on Oversight and Government Reform
Subcommittee on Information Technology

March 7, 2018

Chairman Hurd, Ranking Member Kelly, and Members of the Subcommittee, good afternoon and thank you for the invitation to speak with you. Today, I will be addressing the topic of "Game Changers: Artificial Intelligence and the Federal Government" and sharing with you important aspects of how we are using artificial intelligence-based technologies in research and development (R&D) and more broadly in the Department of Homeland Security (DHS) Science and Technology (S&T) Directorate.

As the R&D arm of DHS, S&T focuses on providing the tools, technologies, and knowledge products for DHS operational components, state and local first responders, and the Homeland Security mission ensuring R&D coordination across the Department for the needs of today and tomorrow. S&T's R&D focus areas cover DHS's core mission areas and use our network of industry, national laboratories, international, academic and other partners to seek solutions for capability gaps and define topics for future research.

Across all DHS mission areas, S&T helps integrate innovative technology into everyday use. S&T works directly with DHS Component operators in the field to understand their unique needs and challenges. S&T partners with federal agencies and international governments, industry, and academia to create and test solutions that help the Nation's homeland security officials prevent, respond to and recover from all hazards and threats. Our goal is to provide real-world solutions in a realistic time frame.

The Benefits and Opportunities of Artificial Intelligence

AI's promise can be seen in the rapid proliferation of many applications across government and the private sector. From a government perspective, it holds the potential for enhanced insight into public service operations and improved delivery of services, including through anticipatory responsiveness to inquiries, discovery of new trends, and automation of internal processes. Examples of AI applications span the gamut from helping people navigate immigration systems, to predicting and pre-empting threats, to making critical infrastructure more resilient against increasing attacks.

For AI to realize its potential, we must overcome several challenges, including the potential for widening the gap between our rapidly-changing technology capabilities.

From the DHS S&T perspective, we believe that the future AI trajectory will proceed in the following three ways:

First, AI technology is increasingly providing us with new knowledge and informing our actions. Fueled by sensors, data digitization, and ever-increasing connectedness, AI filters, associates, prioritizes, classifies, measures, and predicts outcomes, allowing the Federal government to make more informed, data-driven decisions.

Second, algorithms are ingesting and processing ever higher volumes of data. Their complexity, especially in the case of deep learning algorithms, will continue to increase, and we need to better understand how outputs are produced from the set of inputs, which may not be able to be understood or analyzed in isolation.

Finally, private industry is leading the way in AI development, as many see the implementation of AI as a key competitive advantage. The private sector's significant investments and the ability to adopt new AI models and processes faster than the public sector present the government with a key decision point on how to best participate in this growing, but still nascent field. Government should move forward with adoption of emerging technologies such as AI to improve citizen services. Government also plays an important role in promoting research and development. Government should ensure it is informed of developments in the private sector, while continuing to support AI research and development, and promote the use of AI technology to create government efficiencies and enhance the public good.

DHS S&T and Artificial Intelligence

AI is an integral part of several S&T Cyber Security Division (CSD) research projects funded within current resources, which are using AI and machine learning techniques for a variety of purposes, including but not limited to predictive analysis for malware evolution; enabling defensive techniques to be established ahead of a future malware variant; detecting anomalous network traffic and behaviors to inform cyber defensive decision making; and helping identify, categorize and score various adversarial Telephony Denial of Service (TDoS) techniques.

A good example of S&T's work involves demonstration of TDoS protection for a major US bank with a significant impact on its contact center that processes close to 11 million calls per week. The machine learning-based policy engine blocks more than 120,000 calls per month based on voice firewall policies including harassing callers, robocalls and potential fraudulent calls. It also blocks two to three phone-based attacks each month (computer-generation of calls into 1-800 toll free destinations in an attempt to collect a portion of the connection or per-minute charges associated with the call). This same technology can be used by 911 call centers to defend against denial of service attacks.

Another S&T research example capitalizes on the convergence of technologies such as machine learning, software defined networking, and global internet routing to help build more robust defenses against Distributed Denial of Service (DDoS) attacks. This specific application uses machine learning to create fine-grained, temporal traffic models that allow anomaly detection without preset thresholds and with low false positive rates. It then uses Software Defined Networking technology to deploy thousands of rules to instantly defend against complex DDoS attacks at very high speeds.

S&T Engaging DHS Components and Startups

DHS S&T launched its Silicon Valley Innovation Program (SVIP) to keep pace with the innovation community and engage that community to tackle significant problems faced by the Department's operational missions. SVIP expands DHS S&T's reach to find new technologies that strengthen national security.

Through a streamlined application and pitch process leveraging Other Transaction Authority, SVIP is seeking solutions to challenges that range across the entire spectrum of the homeland security mission space, including cybersecurity and technology solutions for Customs and Border Protection (CBP) and first responders.

SVIP and AI

DHS SVIP and CBP are working together to evaluate and implement innovative methods -- to include the use of AI and machine learning -- to exchange information and intelligence, build capacity, and increase worldwide security and compliance standards in support of CBP and its international partners. These efforts widen border security capabilities and support a "defense in depth" approach to combat the global threat environment, and strengthen our combined enforcement efforts.

CBP offers advanced passenger data-screening and targeting technology as an open source software project, known as the Global Travel Assessment System or GTAS. It is a turn-key application that provides to CBP's foreign counterpart agencies the necessary decision support system features to receive and store air traveler data, both Advanced Passenger Information (API) and Passenger Name Record (PNR), provide real-time risk assessment against this data based on a country's own specific risk criteria and/or watch lists, and view high-risk travelers as well as their associated flight and reservation information. The purpose of GTAS is to provide border security entities the basic capacity to ingest, process, query, and construct risk criteria against the industry-derived standardized air traveler information. The system provides border security organizations with the necessary tools to prescreen travelers entering into and leaving their countries.

Last year, DHS SVIP and CBP partnered to enhance the GTAS project with solutions from the global innovation community, namely new capabilities using AI and machine learning, and identifying the following three capabilities for consideration:

VISUALIZATION: This would extend the basic flight and passenger tabular list screens with geospatial, link analysis, seat map visualization, or any other concepts that improve the software by presenting data graphically

PREDICTIVE MODELS: These would complement GTAS rules engine with statistical and machine learning models and a "predictive model engine" that performs real-time risk assessment and

ENTITY RESOLUTION: This capability would enhance the basic name/date of birth and document matching algorithms to support more advanced entity identification and matching algorithms

A Path Forward
DHS continues to support the design of AI systems in a manner that makes the actions and decision-making of technologists, government officials, and other users both transparent and understandable. The design, development, implementation, and evaluation of AI solutions should generate trust that the government and industry are innovating responsibly, by demonstrating that the government is balancing risks in delivering on its mission to serve the public fairly and justly, and influence responsible evolution and the role for AI in the private sector.

Innovation in AI should be advanced through an emphasis on responsible R&D. In addition, AI R&D should involve multidisciplinary perspectives that involve experts from computer science, and other physical and social sciences.

In order for the Government to be relevant in this fast moving and competitive future that is being defined by AI, the following notions are essential: the use and development of datasets for AI R&D, strategic communication and engagement with industry on relevant considerations, and the development of trust in applications of AI.

Summary
Mr. Chairman and Members of the Subcommittee, as you heard in your Hearing last month, AI is here to stay. It is no longer a dream from decades past. It is being used for many applications in the private sector and Government and we are only at the beginning of understanding all its possible opportunities.

AI and machine learning are rapidly moving from scientific understanding to engineering application in most domain areas. This reality means DHS must aggressively work with its research, development, test and evaluation partners throughout government and industry to develop effective, trusted homeland security applications of AI and machine learning. This requirement includes strong working relationships with industry, so homeland security applications can leverage the best of industrial innovation, and homeland security capabilities can continue to support the strengthening and growth of American economic capabilities. These efforts must necessarily contribute to key areas of challenge – cyber security, screening people and cargo, risk understanding throughout the nation's critical infrastructures, valuable investment in smart infrastructure and operations – all critical missions of DHS.

Thank you for your thoughtful leadership on these issues and I look forward to your questions.

APPENDIX: National Artificial Intelligence Research and Development Strategic Plan

The National Artificial Intelligence Research and Development Strategic Plan, National Science and Technology Council, Networking and Information Technology Research and Development Subcommittee, October 2016, https://www.nitrd.gov/PUBS/national_ai_rd_strategic_plan.pdf.