Testimony of

WILLIAM BRYAN
Senior Official Performing the Duties of the
Under Secretary for Science and Technology Directorate
Science and Technology Directorate
U.S. Department of Homeland Security

House Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation
March 11, 2020

Good Afternoon Chairman Richmond, Ranking Member Katko, and distinguished members of the subcommittee. Thank you for inviting me here today to testify on the President's Budget Request for Fiscal Year (FY) 2021, which includes a request of $643.7 million for the Science and Technology Directorate (S&T) within the U.S. Department of Homeland Security (DHS).

S&T's research and development (R&D) activities support a broad range of DHS missions, including domain threat awareness, delivering mitigation strategies, and creating novel technology and approaches for the Components, first responders and other partners across the homeland security enterprise. Our customers put their lives on the line every day to keep our nation safe, and having the correct tools, techniques, and/or technologies can be vital to the operators' safety and success.

We must enable efficient, effective, and secure operations across all homeland security missions by applying timely scientific, engineering, and innovative solutions through research, design, test and evaluation, and acquisition support. This is how S&T delivers results. Technology innovation cycles are rapidly changing and the nature of the threats we see is dynamic. This combination presents a significant challenge to traditional R&D approaches as well as meeting Component requirements and needs in a fiscally constrained R&D environment. S&T is less than 1 percent of the entire federal R&D budget – and we strive every day to get as much value out of those funds as possible.

Therefore, it is my responsibility to ensure an efficient, effective, and nimble organization is in place to address R&D needs of Homeland Security front line operators, particularly the DHS operational Components and first responders, today and into the future. Either through the identification of existing technologies or the timely development of new technology, S&T can provide them with the tools they need to safely and effectively protect the Homeland and the American people. Under my leadership S&T has strengthened our relationships with our customers, the DHS operational components and first responders, to provide impactful solutions to those on the front line. We continue to solidify and strengthen S&T's core capabilities and provide a deliberative approach to program execution that ensures timely delivery and solid return on investment for our nation's taxpayers.

S&T has become more agile and responsive, ready to move quickly in response to changes in the threat environment, and makes use of existing technologies, when available, that can be adapted

and leveraged to expedite the development of vital capabilities. S&T has significantly enhanced its ability to transfer capabilities to where they are most needed by working closely with operators, component partners, and industry to deliver effective solutions. The revitalized S&T has strengthened its relationships with DHS components, first responders, and other customers, and results in a more integrated approach to innovation, requirements gathering, and problem solving. At a strategic level, S&T has created a capability to identify, prioritize and report on emerging technology risks facing the United States. Together with DHS Policy, S&T will identify and assess emerging technologies most likely to significantly improve operations and/or threaten the DHS mission over the next two –to five years. Results will support Senior DHS executives as they prioritize the list of technologies and shape the DHS investment portfolio to address risk.

A strong cross-Department Cybersecurity R&D program is critical for DHS. The Cyber Security & Infrastructure Security Agency (CISA) and S&T have made tremendous strides in resetting the relationship, directing R&D resources into mission support of CISA requirements. CISA and S&T have established repeatable processes to identify capability gaps, prioritize needs, and execute on RD&I needs. The FY 2021 Cybersecurity R&D budget request is for $24 million and places all Cyber R&D funding with S&T.

S&T is currently partnered with the National Institutes of Artificial Intelligence (AI) with the goal of mitigating risks to misuse of AI, identifying opportunities and applications of AI within the homeland security mission space, improving privacy protection, and developing new governance and policy frameworks for artificial intelligence and machine learning. S&T is working with its operational DHS Component partners to assess opportunities for leveraging Automated Machine Learning (AutoML) and related data preparation tools as a means of accelerating understanding and use of this technology within the DHS enterprise. In FY 2021, S&T will examine and characterize the state of artificial intelligence research relative to future homeland security mission applications. Research activities will focus on the development of core capabilities that enable trustworthy artificial intelligence to improve core automation capabilities that are secure, private, and trusted for critical homeland security applications.

The FY 2021 Budget request provides $14.4 million for S&T's Probabilistic Analysis for National Threats Hazards and Risks (PANTHR) program that aligns S&T's chemical and biological hazard awareness and characterization activities to provide timely accurate and defensible decision support tools and knowledge to stakeholders. PANTHR is currently supporting the Countering Weapons of Mass Destruction Office (CWMD) to address the ongoing Coronavirus outbreak by providing consolidated up-to-date information regarding the virus to DHS components. PANTHR is currently leveraging the capabilities of one of the DHS laboratories, the National Biodefense Analysis and Countermeasure Center (NBACC), which is addressing pertinent scientific questions and DHS operational concerns regarding Coronavirus surface stability and decontamination. PANTHR funding in FY 2021 would further support the expansion of these national capabilities to address current and emerging chemical and biological concerns. Additionally, the FY 2021 request would allow PANTHR to develop additional assessment capabilities to address growing infrastructure concerns, such as the bio-economy, and fill other critical technical hazard data gaps regarding WMD risks to the Homeland.

S&T is requesting $35.9 million in the FY 2021 budget to directly address Customs and Border Protection (CBP), the U.S. Coast Guard (USCG), the U.S. Secret Service (USSS), and the Federal Protective Service (FPS) requirements for Countering Unmanned Aircraft System (CUAS) requirements. In close coordination with our operational customers, S&T is responsible for the initial CUAS deployment architecture, technology selection, system integration, system test, training and cyber compliance. The FY 2021 S&T CUAS investment will focus on mission interoperability with the Department of Defense and Department of Justice in the National Capital Region, improved CUAS capabilities for DHS components, and addressing future threats. UAS threats to critical infrastructure and security activities will likely increase in the near future as the number of UAS introduced into the national airspace continues to increase. However, currently the use of technical means to detect, track, and disrupt malicious UAS operations remains limited.

S&T is dedicated to developing or adopting innovative tools for DHS Components, and the FY 2021 Budget request supports that effort. For example, the S&T Opioid Detection project continues to integrate advanced technologies, including narcotics anomaly detection algorithms and chemical sensing technologies, into CBP international mail facilities, and to evolve efforts directed at detecting synthetic opioids in additional operational environments in response to changing trafficking dynamics. Increased funding will also further improve the understanding of supply chain logistics and intelligence to aid in targeting, investigations, and ultimately, disruption of international smuggling. The administration is also focusing on Targeted Violence and Terrorism Prevention, and S&T is a vital partner using research to inform policy, strategy, tactics, techniques and procedures. S&T is actively working to support technology integration and techniques to reduce the likelihood of mass violence and improve the ability to prevent and respond to a mass violence event.

The FY 2021 request continues support for S&T's Silicon Valley Innovation Program (SVIP) at $10 million, which leverages innovative commercial capabilities from across the country through non-traditional government contractors to rapidly deliver technology to fulfill DHS component defined requirements. This program fosters rapid development and delivers tested technology into the field in a much shorter timeframe than is possible under traditional vehicles. S&T's SVIP collaborates with DHS operational components to provide solutions that enhance overall situational awareness, detection, tracking, interdiction, and apprehension.

To date, S&T's SVIP has awarded $18M in funding and processed over 485 applications across 14 topic areas. S&T has worked with 49 small start-up companies from 15 different states and leveraged over $500 million in private sector investment that aligns ongoing private sector activity with DHS operational component requirements. SVIP has successfully transitioned 3 technologies into CBP operational environments including a new generation of radar to support U.S. Border Patrol operations. This radar technology was incorporated into 58 Border Patrol towers on the Southwest border and a similar amount are planned for transition in 2020.

The FY 2021 Budget request adds a Procurement, Construction and Improvements account to address the decontamination and closure of the Plum Island Animal Disease Center. S&T is on time and on budget to complete the construction of the National Bio and Agro-Defense Facility (NBAF). This state of the art facility will be transferred to the U.S. Department of Agriculture

upon completion of construction and will be the Nation's only Bio Safety Level 4 laboratory that is capable of studying large animal diseases in livestock, such as African Swine Fever and Foot and Mouth Disease. After NBAF is completed, the Plum Island facility will require decontamination. The $18.9 million of the FY 2021 request will begin decontamination activities and stand up the program office to manage this multi-year effort.

The FY 2021 Budget request supports S&T's Office of University Programs in two vital efforts, our Centers of Excellence (COE) and working with Minority Serving Institutions (MSI).

The FY 2021 Budget request allows for the continuation of the University-based COEs that are focused on homeland security mission needs. COEs that will receive funding in Fiscal Year 2021 will conduct research and development that aligns with the Administration's priorities to strengthen border security, cyber security and infrastructure protection, and prioritize trans-national criminal investigations. S&T conducts rigorous evaluations of each Center's performance using established criteria to help inform project funding decisions that meet operator needs and stay focused on transferring or transitioning research and technology outputs into field use.

S&T seeks to leverage and utilize the unique intellectual capital in the MSI community to address current and future homeland security challenges and to provide relevant learning opportunities to diverse and highly talented individuals and inspire the next generation of dedicated to homeland security professionals. Our efforts provide learning opportunities for students that already are pursuing Science, Technology, Engineering and Mathematic (STEM) related degrees. These awards support MSIs in their efforts to attract highly technical students and provide exposure and mentorship opportunities with DHS programs. S&T's efforts with MSIs are important for ensuring students develop the cross-functional skills essential to their flourishing and meeting the demanding needs of the homeland security missions. By establishing continuous relationships between COEs, MSIs, DHS component agencies, and private-sector entities, S&T is expanding partnering institutions and providing resources needed for students to gain meaningful work experiences that prove invaluable to the growth of their careers in homeland security related areas.

S&T's mission is to deliver effective and innovative insight, methods, and solutions for the critical needs of DHS Components and our operational partners in homeland security.

Chairman Richmond, Ranking Member Katko, and members of the Committee, thank you again for the opportunity to appear before you today and for your continued support of S&T.

I look forward to answering your questions.