Statement of Jacob Parker
Director of Government Relations
Security Industry Association

Before the

United States House of Representatives
Committee on Homeland Security
Subcommittee on Emergency Preparedness, Response and Communications

How Effective is the Science and Technology Directorate?: Stakeholder Perspectives

November 7, 2017

HVC-210 Capitol Visitors Center

Good morning Chairman Donovan, Ranking Member Payne and distinguished members of the Subcommittee. I am Jake Parker, Director of Government Relations for the Security Industry Association, a non-profit international trade association representing nearly 800 companies that develop, manufacture and integrate security solutions, and employ thousands of technology leaders.

Thank you for the opportunity to testify before you today on the partnership between the U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T) and its stakeholders in the private sector. The input I am providing is based, broadly, on the experiences and perspectives SIA member companies have shared with me, which include both small companies and large corporations.

Technology provided by the security industry plays a key role in DHS component operations, and in protecting critical infrastructure such as chemical facilities, airports, seaports, mass transit systems, the energy sector, federal offices and even K-12 schools and universities.

Since November is Critical Infrastructure Security and Resilience Month, I want to first highlight S&T's work through the Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act Office, which is the most common interface between SIA member companies and the Directorate. As you know, the SAFETY Act of 2002 established a process to encourage the development and widespread deployment of security technologies addressing the terrorist threat by providing liability protections for qualified providers against claims arising from terrorist attacks. The potential for such claims was identified as major obstacle to the deployment of effective security solutions following the attacks of September 11th.

From our point of view, the program has been a major success and a catalyst for adoption of new technology in many ways. The private sector owns and operates the vast majority of critical infrastructure in the United States. Not only does the SAFETY Act protect these end users from liability for deploying technology, SAFETY Act designation and certification provides a level of assurance that a product or system meets high standards of safety and effectiveness, and works as intended.

Our industry provides manufactured products, and well as systems integration services and software such as cybersecurity programs - all of which are potentially eligible for SAFETY Act designation or certification. In addition, owners or operators of critical infrastructure are making increasing use of the SAFETY Act designation for their comprehensive security programs, in which security technology plays a key role.

According the SAFETY Act Office, during FY17, 91 applications were approved out of 133 submitted, taking an average of nearly four months to get through the process. The Office projects that approval of these technologies will support 87,000 jobs and significantly increase revenue for providers.

We believe that Congress should work to ensure this important program continues, and importantly, is provided with the resources necessary to meet demand. Specifically, Congress should provide the SAFETY Act Office with a line item appropriation. This will provide budgetary certainty and program continuity, as well as help measure the return on investment.

As far as the broader array of S&T programs, we are encouraged with recent signs the Directorate is strengthening efforts to better coordinate research and development (R&D) activities across DHS

components and with industry stakeholders. Two years ago, when Dr. Brothers – who we are honored to have with us here today – was serving as Under Secretary, Integrated Product Teams (IPTs) were re-established to track and harmonize department-wide research and development efforts between S&T and the components. The most recent IPT report for FY17 is based upon only the second round of data gathering across DHS components, as well as a new process for involving operational components in the identification of capability gaps on which to focus R&D efforts. IPTs are aimed at sustaining a year-round process in which a designated component "shepherds each gap from the identification of needs to the transition of solutions to close the gap" according to the report.

In gathering feedback from our member companies, a recurring theme was the importance of bolstering the business case for participation in S&T programs. Our members tell us that for S&T programs to be truly successful from their standpoint, each effort needs to be of championed by a DHS operational component, and accompanied by some form of commitment to make use of the technologies being explored if the government is the intended end user. The component should have some level of involvement in the project being executed from the beginning of the process, and prior to making any significant expenditures.

There is a perception among some in the industry that S&T programs only infrequently significantly impact the operational or procurement activities of the DHS components, even with a successful engagement. For this reason, the choice may be made to devote more time and resources to focus primarily on relationships with the program offices on the component side.

More involvement from the components up front could help address this perception, as well as efforts to increase industry awareness of S&T's new initiatives. Last month, S&T released its new Industry Guide, which very effectively summarizes current needs and programing, providing a future R&D outlook and linking industry to each of the ways to participate. We understand from discussions with personnel at S&T that they are working towards a providing a centralized online interface for industry to pull together information about opportunities that is currently listed in disparate locations.

Successful engagement with industry also depends on the business model of companies that possess the expertise S&T is seeking. For many smaller companies, the topic often needs to be aligned with something they are already doing to justify the use of resources to apply, especially those with limited experience with grant proposals and similar processes. S&T should do everything possible to simplify and streamline the process to make it easier for companies that do not have this expertise to participate.

Whether large companies or small, industry would benefit from making the process of working with S&T easier and less bureaucratic. This is one reason we are optimistic about plans to update and improve S&T's Long Range Broad Agency Announcements (LRBAA) process. We understand that early next year S&T is planning to make significant changes to the process based on in industry feedback, as LRBAAs are initiated for 2019 and beyond. This includes a clarification of priorities that are linked directly to component needs, a simplified and streamlined application process, increased communications with program managers prior to submission, shortened review time as well as feedback to submitters. This feedback is particularly important for accepted proposals that are unfunded, to increase the chance of success with future submissions. Further, we think the evaluation process can be improved to the extent it can be aided by personnel with product development experience.

As you know, the government is challenged by the fact that technology is now evolving so quickly that it often outpaces traditional government R&D and acquisition vehicles. Meanwhile, technology-based solutions are more important than ever to achieving DHS component missions. According to the 2017 S&T Innovation Strategy, among the Directorate's goals are to ensure that industry applies its resources toward meeting the demands of the Homeland Security Enterprise (HSE), as well as to ensure that technology end users are more satisfied with products available on the commercial market.

When it comes to the S&T R&D investment outlook for the next four years, the security industry is poised to contribute significantly, particularly when it comes to priority areas like biometrics collection and utilization, robotics and autonomous systems, enhanced situational awareness, identity credentialing and access management, automated vetting and other technologies.

SIA and S&T have maintained a memorandum of understanding (MOU) that facilitates information sharing on the adaptation of electronics-related technological innovation for use at the federal, state and local level for homeland security applications. SIA is committed to continuing to do our part to facilitate the participation of our industry in helping meet HSE needs, and we look forward to working with S&T in new and more effective ways in the future as new leadership is appointed.

On behalf of the Security Industry Association, I appreciate the opportunity to provide collective input from our industry on working with S&T. I will do my best to answer any questions you may have, however if there is any information requested I cannot provide today, I will be happy to work with our members to provide helpful responses.