



Homeland Security Advisory Council

Homeland Security Technology and Innovation Network

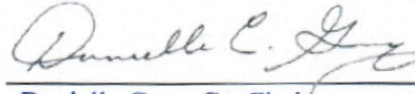
Final Report

March 16, 2023

This publication is presented on behalf of the Homeland Security Advisory Council, Homeland Security Technology and Innovation Network Subcommittee, Co-Chaired by Carrie Cordero and Danielle Gray to the Secretary of the Department of Homeland Security, Alejandro N. Mayorkas.



Carrie Cordero, Co-Chair
Senior Fellow & General Counsel
Center for New American Security



Danielle Gray, Co-Chair
Executive Vice President,
Global Chief Legal Officer,
Walgreens Boots Alliance, Inc.

This page is intentionally left blank.

TABLE OF CONTENTS

HOMELAND SECURITY TECHNOLOGY AND INNOVATION NETWORK SUBCOMMITTEE MEMBERS	5
HOMELAND SECURITY ADVISORY COUNCIL STAFF	5
EXECUTIVE SUMMARY	6
METHODOLOGY	7
RESEARCH & ANALYSIS	9
RECOMMENDATIONS	15
CONCLUSION	17
APPENDIX 1: TASKING LETTER	18
APPENDIX 2: SUBJECT MATTER EXPERTS AND OTHER WITNESSES	23
APPENDIX 3: DHS INNOVATION OFFICES	24

**HOMELAND SECURITY TECHNOLOGY AND INNOVATION NETWORK
SUBCOMMITTEE MEMBERS**

Carrie Cordero, Co-Chair	Senior Fellow & General Counsel Center for New American Security
Danielle Gray, Co-Chair	Executive Vice President Walgreens Boots Alliance, Inc.
Marc Andreessen	Co-founder and General Partner Andreessen Horowitz
Leon Panetta	Former Secretary of Defense and Chairman The Panetta Institute for Public Policy
Karen Tandy	HSAC Vice Chair, Administrator (Ret.) Drug Enforcement Administration
Michael McGarry	Vice President, Governance and Risk Walgreens Boots Alliance, Inc.
Matthew Shortal	Operating Partner Andreessen Horowitz

HOMELAND SECURITY ADVISORY COUNCIL STAFF

Rebecca Kagan Sternhell	Executive Director
Joseph Chilbert	Senior Director
Alexander Jacobs	Senior Director
Carley Bennet	Student Intern

EXECUTIVE SUMMARY

The Department of Homeland Security (DHS or the Department) faces a constantly evolving threat landscape fueled by rapidly advancing technology. To keep pace with new threats and protect the nation's security, the Department needs a robust and efficient Homeland Security Technology and Innovation Network that encourages an enhanced schedule of development and deployment for critical technology and assets. Building this network requires strong partnerships with different stakeholders, especially those from the private sector.

In October 2022, the Secretary of Homeland Security tasked the Homeland Security Advisory Council with forming a subcommittee to assess the private sector experience, especially regarding technology development and innovation, and with providing recommendations on how the Department can create a more robust and efficient Homeland Security Technology and Innovation Network. The Homeland Security Advisory Council formed the Homeland Security Technology and Innovation Network (HSTIN) Subcommittee to respond to the following tasking:

1. An assessment of how the private sector engages with the current R&D and acquisition programs and opportunities, including where those can be maximized or improved.
2. Recommendations on different means of increasing innovative technology partnerships with the private sector.
3. Recommendations on how to harmonize existing innovation efforts across the Department and its components to best leverage funding and resources.
4. Identification of current barriers to developing a more robust technology and innovation network, including legal, contracting, and policy considerations.

From December 2022 to March 2023, the Subcommittee met with representatives from the DHS Science and Technology Directorate (S&T), DHS Private Sector Office (PSO), as well as the following DHS Components: Customs and Border Protection (CBP), Transportation Security Administration (TSA), Immigration and Customs Enforcement (ICE), and U.S. Coast Guard on their innovation efforts. The Subcommittee has identified seventeen offices spread across eleven offices or components that include "innovation" as all or part of their function across the Department. See Appendix 3. In addition, the Subcommittee met with representatives from the private sector and conducted additional research.

The Subcommittee determined that DHS could improve its innovation, research and development, and technology network with the private sector by adopting the following recommendations:

1. Create a concise, "How to Work with DHS: Focus on Mission" Guide to serve as a roadmap for points of entry, contract vehicles, special contracting opportunities, and points of contact within each component.
2. Develop a process for prioritizing technology innovation projects across the Department; appoint a senior advisor within the Secretary's office to coordinate and manage innovation projects across the Department; and develop an online dashboard, or tool that will assist DHS

leadership track progress on innovation projects.

3. Leverage best practices by taking a close look at various offices across the Department that claim responsibility for driving innovation with an eye toward reducing redundancy.
4. Direct more deliberate actions to measure progress on innovation and funding initiatives by adding structured metrics and accountability.
5. Conduct an internal review of contracting authority and processes for mission-supporting technologies. The review should be conducted to identify processes that can be streamlined, legal and regulatory requirements that can be clarified and legislative remedies that may be appropriate to seek from Congress.

METHODOLOGY

The Homeland Security Technology and Innovation (HSTIN) Subcommittee drew upon expert interviews and supplemental research from December 2022 to March 2023. In particular, the Subcommittee met with representatives, subject matter experts and leaders from the DHS Science and Technology Directorate (S&T), DHS Private Sector Office (PSO), representatives from the private sector, as well as the following DHS Components: U.S. Customs and Border Protection (CBP), Transportation Security Administration (TSA), Immigration and Customs Enforcement (ICE), and the U.S. Coast Guard (USCG) on their innovation efforts. These briefings were valuable and provided background information to inform our recommendations.

The Subcommittee also sent out a request for information (RFI) to the following components requesting specific information on how their innovation efforts interact with the private sector: CBP, TSA, ICE, USCG, the Federal Emergency Management Agency (FEMA), and U.S. Secret Service (USSS). In addition, to gain an outside perspective, the Subcommittee met with members of industry to provide their perspectives on working with DHS and component agencies.

As part of its efforts, the Subcommittee focused on how DHS can improve its efforts to engage with start-up companies that drive the innovation network and technology sector in the country. The Subcommittee approached this project from the perspective that large, well-established contractors already have demonstrated abilities and experience navigating the federal acquisition arena, including at DHS. The Subcommittee excluded from its review how the well-known prime or major federal contractors in the homeland security space work with the Department. Similarly, the committee did not address procurement issues as they relate to non-technology related vendor services for the Department that are ancillary to core mission or operational activities (i.e., service providers).

The Subcommittee's overarching interest was in evaluating how specific DHS components and DHS Headquarters, interact with and provide avenues for technology-related start-up companies to leverage their products and capabilities to serve various high priority DHS mission sets. Overarching themes from the briefings the Subcommittee received were that (i) the three-to-five-year procurement process has a significant impact on the speed of innovation, and (ii) that each operational component navigates the procurement process and its innovation activities relatively independently and with varying success as it relates to acquisition of new technologies. **The Subcommittee's recommendations primarily**

address this second issue: how the Department can better support, bolster, and streamline its innovation related efforts in a way that maximizes opportunities for non-traditional companies to enter the market, prioritizes innovative acquisitions, and reduces barriers to entry. The Subcommittee has made one recommendation related to the first issue, but extensively reviewing the procurement process and accompanying legal and regulatory frameworks was beyond the scope of the Subcommittee's work.

RESEARCH & ANALYSIS

Innovation efforts across the national and homeland security space in the federal government exist at varying levels of breadth and sophistication, and DHS as an enterprise has a mixed approach to harnessing innovative tools to support its mission. Elsewhere in the national security federal government enterprise, the Defense Department's Defense Advanced Research Projects Agency (DARPA) and the intelligence community's parallel entity, Intelligence Advanced Research Projects Activity (IARPA), are entities focused on cutting edge research and development to meet over the horizon challenges. In addition, the Defense Innovation Unit (DIU) is the Defense Department's component specifically dedicated to "accelerating commercial technology for national security."¹ And individual services in the military also have innovation-focused components, such as Army Futures Command or the Air Force's AFWERX. DHS as a Department has no such parallel to these specific entities in other parts of the national security enterprise. Having just passed the twenty-year mark of the Department's existence, DHS is still in the early stages of charting a path to most efficiently acquire new technologies to support its mission in a way that conforms with legal and regulatory requirements and is timely.

It is critical to acknowledge that the challenges faced by DHS to effectively navigate its mission needs in connection with a rapidly evolving global technology landscape are far from unique in the federal government; instead, the challenges DHS faces in this area are consistent with the imperative to modernize how much of the federal government leverages 21st century technology developments. Redesigning long standing bureaucracies in order to develop a comprehensive U.S. technology strategy are a whole-of-government challenge, not just a DHS challenge.² For example, the Department of Defense has surged its efforts, with congressional support, to more effectively lead technological change and innovation across the Department's activities.³ DHS has the added challenge of having generally ranked on the low end of federal agencies' budget commitments to research.⁴

New technologies that can support both defense and homeland security missions are increasingly driven by research and development conducted outside of government. As former researchers at the Center for a New American Security articulated in a policy paper on the development of a U.S. technology strategy, "the U.S. government is no longer the locus of American technology innovation, it will need agility in its processes to exercise relevance vis a vis private sector developments."⁵ And, as former Google CEO Eric Schmidt recently wrote, the "trifecta of government, industry and academia" that was the "primary source of American innovation" has receded as federal dollars

¹ <https://www.diu.mil/>

² Loren DeJonge Schulman and Ainikki Riikonen, *Trust the Process: National Technology Strategy Development, Implementation and Monitoring and Evaluation*, Center for a New American Security (April 20, 2021) <https://www.cnas.org/publications/reports/trust-the-process>.

³ Statement for the Record of Barbara McQuiston, Defense Innovation and Research, U.S. Senate Appropriations Committee, Committee on Defense, April 13, 2021, <https://www.appropriations.senate.gov/imo/media/doc/McQuiston%20Statement%20for%20the%20Record.pdf>.

⁴ Nate Bruggeman and Ben Rohrbaugh, Closing Critical Gaps that Hinder Homeland Security Technology Innovation, Belfer Center for Science and International Affairs, Homeland Security Policy Paper, April 2020, <https://www.belfercenter.org/sites/default/files/files/publication/HSP%20paper%20series%205-2.pdf>.

⁵ Loren DeJonge Schulman and Ainikki Riikonen, *Trust the Process: National Technology Strategy Development, Implementation and Monitoring and Evaluation*, Center for a New American Security, April 20, 2021, <https://www.cnas.org/publications/reports/trust-the-process>.

devoted to research and development have decreased, and private investment to spur innovation has stepped into fill the breach.⁶ Accordingly, federal government agencies and personnel need to adjust in real time to the changing budgetary, capital market, and technology industry environments.

Industry is actively engaging in efforts to improve the reach of new and emerging technologies into the federal government space. This is due, in part, to the fact that technological innovation is originating outside government, which can be attributed to both creativity and innovation inherent in the technology start-up community, as well as the reduction in federal government funding for research and development. Federal government funding for research and development is far less than it was in the mid-20th century.⁷ The Strategic Competitive Studies Project, chaired by Schmidt, released a report in the fall of 2022,⁸ which articulates how the use of venture capital and private financing to fund technology innovation can serve as an alternate model from federal government-funded research and development. This approach upsets the historical or traditional federal government operating assumption which is that federal government research and development requires more funding for those efforts. The network of technology-focused venture capital leaders views private dollars as the way to fund big technological change the government needs.⁹

The Subcommittee conducted virtual research roundtable interviews and discussions with several headquarters offices and DHS operational components that include innovation efforts and initiatives among their responsibilities. Subject matter experts whom the Subcommittee engaged with can be found in Appendix 2. In addition, the Subcommittee received input from several industry representatives in the start-up space. The Subcommittee also sent formal Requests for Information (RFIs) via the HSAC staff to the following components and received written submissions in response to those requests: CBP, FEMA, ICE, TSA, USCG, and USSS. The following component-specific information was derived from these interviews and briefings:

Science and Technology Directorate (S&T)

The DHS Science and Technology Directorate (S&T) is the Department's science advisor and research and development arm. S&T and DHS as a whole recognize that DHS must partner with the industry for successful innovation. S&T received mixed reviews among some industry, with positive comments about its industry rallies and concerns that its postings need to be clearer with full insight into the process that it will follow. Started in 2018, the S&T Rally challenges industry to develop faster, more accurate, and easier-to-use biometric recognition capabilities to improve security and ease of use at security checkpoints.¹⁰ Some of the pros identified from the rallies were that they provide an opportunity to demonstrate innovative technology and identify concerns or areas that need improvement. In addition, they provide the vendor community with a signal towards the types of technologies DHS is looking towards in the future, and they allow vendors to engage directly with key

⁶ Eric Schmidt, *Innovation Power: Why Technology Will Define the Future of Geopolitics*, Foreign Affairs, March/April 2023.

⁷ John Costello, Martijn Rasser and Megan Lamberth, *From Plan to Action: Operationalizing a U.S. National Technology Strategy*, Center for a New American Security, July 29, 2021, <https://www.cnas.org/publications/reports/from-plan-to-action>.

⁸ *Future Tech Platforms Interim Panel Report*, Strategic Competitive Studies Project (SCSP) (2022) <https://www.scspp.ai/about/>.

⁹ Katherine Boyle, *Building American Dynamism*, January 14, 2022, <https://a16z.com/2022/01/14/building-american-dynamism-2/>.

¹⁰ Biometric Technology Rally <https://www.dhs.gov/science-and-technology/biometric-technology-rally>

stakeholders from the government. Some areas for further improvement include a post event action plan to determine what worked and what did not. Also, a broader education/marketing campaign is needed for biometric technologies geared toward outside stakeholders that may be skeptical of the technology.

Industry also noted experiencing a disconnect between S&T and the components regarding priorities and investment. For its part, S&T identified several core challenges DHS faces in setting an R&D agenda, including the vast diversity of missions across the components, a lack of visibility into the work and efforts of individual components, and the tendency to conduct near-term innovation efforts as opposed to the projects with longer time horizons. S&T also advised that there is currently a limited DHS R&D budget. Within S&T, its budget is divided 65-70% for near term immediate needs, with the 35% balance devoted to longer term projects. For FY23 Federal R&D Budget Requests, DHS ranks 11 of 14.¹¹

Across the Department, awareness of S&T's opportunities and support of DHS could be improved through better coordination and communication, although components do participate collaboratively in a monthly R&D steering group. S&T is involved in ensuring federally funded technologies are moved out into the marketplace for the first responder community through programs such as Commercialization Accelerator Program, Partnership Intermediary Agreements, or Technology Transfer and Commercialization. S&T advised that current challenges for coordinating DHS R&D across the Department include: diverse mission sets across components and the homeland security enterprise; diverse cultures, internal processes, relationships; agency specific appropriations; loosely aligned R&D, requirements, and acquisition processes; lack of visibility and transparency into Department-wide R&D; and a tendency to focus on near-term needs vs long-term.

DHS currently employs a “hybrid” system of short-term innovation efforts conducted within each of the components, and longer-term research and innovation projects led by S&T. The Subcommittee’s review revealed that there could be greater clarity from the top down as to what constitutes short- and long-term innovation projects. For example, DHS, even at S&T, does not appear to be focused on far over the horizon innovation initiatives such as greater than five years out. This may be appropriate given the mission and operations of DHS, however, greater clarity across DHS components and S&T as to how the Department defines short- and long-term investment, research, development, and planning, would be useful.

CBP Innovation Team (INVNT)

The CBP INVNT has established itself as having a reputation in the start-up technology community for successfully navigating the procurement process in favor of leveraging innovation. Its success in this area is likely due to several factors. First, CBP uses specific legislative authorities that enable it to fast-track projects up to \$25 million (formerly \$10 million).¹² INVNT identifies, adapts, and delivers innovative commercial technology solutions in operationally relevant quantities to maximize mission impact and keep front-line personnel safer and more effective. Second, the INVNT group has had

¹¹ Congressional Research Service Federal Research and Development (R&D) Funding: FY2023 <https://crsreports.congress.gov/product/details?prodcode=R47161>

¹² The National Defense Authorization Act, section 880 has been extended to 2027, services have been reinstated, and the threshold increased from \$10M to \$25M. The use of section 880 is now a valid and valuable option for DHS and CBP moving forward.

substantial leadership sponsorship and advocacy at the highest levels, for its work. Third, INVNT appears to have hired personnel who are highly capable at executing their objectives and solely focused on R&D and the transition to acquisition.

A successful avenue INVNT has used has been CBP leveraging the small business innovation research process (SBIR). INVNT staff advised that it has been an effective vehicle through the Small Business Administration. From CBP INVNT's perspective, delegated other transaction authority (OTA) would be beneficial. The INVNT team has worked to leverage a variety of contract vehicles to meet its objectives, including the use of bridge funding and partnership networks to accomplish goals. For example, CBP is leveraging a Space Force contract to support some of their pilot innovation efforts. CBP also intends to leverage a modular contracting process as a Federal Acquisition Regulation (FAR)- based contract vehicle that it will start leveraging here in the near-term future. INVNT strives to work with stakeholders to acquire funding beyond pilot programs.

CBP INVNT advises that it uses a process for transitioning private sector partners from R&D to procurement. INVNT commits to funding two-years of operations and sustainment (in the event funding is available) to provide the receiving organization to get its funding requests into the resource allocation plan and to prepare to take control of the transitioning technology. INVNT works with transition partners at the onset to sign transition agreements to ensure early buy-in prior to technology deployment, or contract award. INVNT leverages strategic contracting vehicles to award technology contracts prior to transition and attempts to provide runway on both period-of-performance and contract ceiling to ensure the receiving partner can seamlessly continue with the technology.

Transportation Security Administration (TSA)

TSA is currently focusing its efforts on creating a culture of innovation throughout the component, which traditionally has not been an entity well situated to work with the startup community. In furtherance of this effort, in October 2022, TSA published its first Innovation Doctrine,¹³ as well as its long-term strategy and capital investment plan, which at least one private sector company encouraged as a model that should be considered DHS-wide. TSA stood up an Innovation Task Force (ITF) to understand an increase in vendor opportunity for benefiting the operational environment. TSA was codified in the FAA Reauthorization Act of 2018¹⁴ with a requirement to conduct field demonstrations, gathering performance data, and understanding how we can influence the requirements and the acquisition programs.

Immigration and Customs Enforcement (ICE)

ICE advised the Subcommittee that the agency is focused on harmonizing and broadening the definition of innovation to make it part of its culture. ICE advised that it does not have a single office within the component that leads innovation activities, however, in 2022 ICE hired its first Chief Innovation Officer, which resides in the ICE Office of Chief Information Officer. For formal R&D efforts, the ICE Office of Investment and Program Accountability, which contains the ICE Component

¹³ https://www.tsa.gov/sites/default/files/12084_layout_tsa_innovation_doctrine_508_final.pdf. The subcommittee notes that a departmental-wide component, such as the Office of Strategy, Policy and Plans, may be an appropriate component to lead the development of a departmental-wide innovation strategy, for consistency and unity of effort.

¹⁴ H.R.302 - FAA Reauthorization Act of 2018 <https://www.congress.gov/bill/115th-congress/house-bill/302/text?q=%7B%22search%22%3A%5B%22PL+115-254%22%5D%7D&r=1>

Acquisition Executive and the Component Requirements Executive, jointly formed a Research and Development Integrated Product Teams Team (IPT) with DHS S&T to collect and prioritize ICE R&D gaps. From ICE's perspective, engagement with the private sector would be the responsibility of DHS S&T for formal R&D efforts.

Within Homeland Security Investigations (HSI) the investigative law enforcement arm as well as the largest arm of the component, several offices or units have innovation responsibilities. In addition, HSI houses the Innovation Lab, which is the agency's centralized hub for the development of new advanced analytics capabilities, tools, and enhanced business processes for HSI. The Innovation Lab strives to create a framework to drive the development of innovative solutions for the agency by taking a "field-first" approach to issues, allowing special agents and criminal analysts in the field to drive the development of these solutions and share insights and feedback with leadership. HSI C3's Child Exploitation Investigations Unit (CEIU) collaborates with private sector industries in the online fight against child sexual exploitation and abuse. CEIU also collaborates with DHS S&T and these private entities to further develop tools and technologies which aid investigators, criminal analysts, and computer forensic analysts in the fight against the exploitation of children.

United States Coast Guard (USCG)

USCG personnel advised the Subcommittee that innovation is a high priority for the USCG and is a particular focus for current leadership. Resources are a significant barrier to USCG efforts to leverage innovation to better support the mission. USCG has limited budget for R&D and relies on DOD, S&T, and additional outside sources to secure funding for projects. USCG has a backlog of projects due to limited budget. There does not appear to be a single-entry point into USCG for industry and no specific guide on how industry can partner with USCG on technology innovation. The primary office for the private sector to work with for R&D and or Innovation is the Office of Research, Development, Test, Evaluation and Innovation (CG-926).

USCG advises that it uses the following process for transitioning private sector partners from R&D to procurement: organizational sponsors are engaged in R&D projects from the outset to ensure transition planning and awareness are considered throughout an R&D project. Sponsors have awareness of project deliverables and reports throughout the course of R&D and are empowered to make support, resourcing, and transition decisions all along the way. Review and process improvement for R&D transitions are ongoing activities in the R&D enterprise in the Coast Guard.

Federal Emergency Management Agency (FEMA)

In response to written requests for information, FEMA advised that FEMA-related R&D activity is sourced and funded through existing DHS S&T contracts. Currently, FEMA has multiple ongoing projects being funded through DHS's Federally Funded Research and Development Centers (FFRDCs). FEMA's Office of Policy and Program Analysis (OPPA) serves as the conduit between FEMA and the DHS S&T/R&D organization. Once DHS approves any project proposals, FEMA's program offices, such as Mission Support and the Office of Response and Recovery, work directly with the DHS FFRDCs. Currently, all R&D-related work for FEMA involves contracts through DHS with the FFRDCs. The products delivered through these contracts is primarily research papers, which generally does not lead to any procurement activity.

United States Secret Service (USSS)

In response to written requests for information, USSS advised that its Office of Investigations (INV) considers its work through universities as the primary “private” entities that USSS engages with for R&D and innovation related to criminal investigations. The USSS Office of Investigations (INV) National Computer Forensics Institute (NCFI) lab is an innovation engine that seeks to partner with universities. The USSS INV NCFI seeks to develop law enforcement sensitive tools and processes to empower SLTT partners in cyber-investigations and cyber forensics. The USSS Office of Strategic Planning & Policy (OSP) Emerging Capabilities Division (ECA) coordinates with private sector companies to identify new technologies. USSS INV advised that has an established process for transitioning private sector partners from R&D to procurement.

USSS advised that NCFI has sought help from commercial partners when a R&D project requires specialized material or equipment. Typically, the specialized material and equipment is proprietary. The NCFI Lab purchases the specialized equipment with the understanding that USSS keeps that company’s intellectual property within the NCFI Lab. For example, USSS is currently utilizing this process for a project focused on ATM jackpotting and ATM malware attacks.

Private Sector Office

The DHS Private Sector Office (PSO) works directly with the Secretary on engagements with private sector entities and industry government relations (GR) teams but is staffed lightly and has little capacity for project management beyond coordinating engagements between the Secretary and industry representatives, groups, or associations. The office does not have a role in the procurement process. Members of the private sector occasionally contact this office for its guidance on component entry points, amounting to approximately 10-15% of its time, reinforcing the need for an agency guide, as called for in recommendation 1, below.

RECOMMENDATIONS

The Subcommittee’s recommendations are focused on how the Department can improve its innovation activities with the goal of supporting critical Departmental missions. As another recent HSAC Subcommittee report recently highlighted, technology is critical to specific operations and activities across the Department that the Secretary and his leadership team is working to improve.¹⁵ It is the view of this Subcommittee, however, that a critical avenue for obtaining the newest technologies that will improve these other aspects of the Department’s work is by leveraging the innovation, flexibility, and adaptability of the network of start-up technology companies building new technologies and applications. Accordingly, the Subcommittee recommends that the Department:

1. ***Create a Concise, “How to Work with DHS: Focus on Mission” Guide.*** This guide should provide a concise roadmap for points of entry, contract vehicles, special contracting opportunities, and points of contact within each component. While there is an in-depth “How to do Business with DHS”¹⁶ presentation available on the Department’s website, in addition to

¹⁵ Homeland Security Advisory Council, Customer Experience and Service Delivery Subcommittee Final Report, December 6, 2022.

¹⁶ https://www.dhs.gov/sites/default/files/publications/how_to_do_business_with_dhs_presentation.pdf

numerous online links and resource pages that dive deep into procurement requirements, companies that do not have experience working with DHS may struggle with identifying points of entry and pathways to developing technology and products that meet mission objectives. There is also a specific guide published by S&T in September 2022.¹⁷ The Subcommittee recommends that DHS develop a simplified guide, tailored to the technology industry, on behalf of the entire Department. This could include, for example, a one-pager that outlines the Department's overall innovation strategy and headquarters-level point of contact and entry, accompanied by a one-pager for each component that outlines critical mission needs and procurement process. The emphasis of these guides should be narrower than a typical "how to work with a federal agency" that is directed to a wide array of service providers and vendors. Instead, the particular guide envisioned by the Subcommittee should focus on the sector of industry that is creating new technologies that can significantly improve the ability of the Department to perform its critical missions.

2. ***Develop a Process for Prioritizing Technology Innovation Projects Across the Department.***

The research and engagement conducted by the Subcommittee revealed the inherent tensions that exist between the authorities and operations of DHS' major components, in connection with the management of the Department at the headquarters level, is highly relevant to the effective functioning of innovation efforts. On one hand, individual components have budgets, authorities, and missions that drive their ability to leverage innovation to achieve their particular mission. On the other hand, DHS leadership should have visibility into what is working or not working across the Department. DHS leadership also has value to add in terms of best use of departmental resources and can guide departmental efforts to eliminate redundancies and prioritize what new technologies and tools will best serve DHS core operational missions. The Subcommittee's assessment is that while there are certain, individual components that are navigating innovation effectively, on balance, the Department would benefit from more prioritization and targeted investment in a few major projects, instead of spreading lower cost projects across the Department. The Subcommittee assesses that major investments across fewer innovative technology solutions may be a better approach.

To achieve that coordination and prioritization, the Subcommittee recommends that the Secretary take a more direct role in managing priorities and championing specific, major projects that leverage innovation to support critical departmental missions. To assist in that effort, the Subcommittee recommends that the Secretary appoint a senior advisor within the secretary's office to coordinate and manage innovation projects across the Department, including reducing redundancies. Development of an online dashboard available to DHS senior leadership that charts status and progress on innovation projects across the Department would be a useful tool.

3. ***Reduce Redundancies and Leverage Best Practices.*** The Subcommittee recommends that DHS leadership take a close look at the various offices across the Department that claim responsibility for driving innovation, with an eye toward reducing redundancy. Some innovation offices, such as within CBP, are focused on rapidly acquiring new technologies with appropriate attention to acquiring new technologies that meet mission needs. Other innovation offices emphasized in their briefings to the Subcommittee, instead, efforts on thought leadership and culture change geared toward innovation. For government, the

¹⁷ [S&T Partnership Guide | Research Priorities and Collaboration Opportunities](#)

Subcommittee recommends that innovation offices focus more on results than on theory. Tangible, measurable successes from innovation efforts in particular components should be regularly briefed to other components and across the Department so that lessons can be learned and shared across the Department.

4. ***Add Structured Metrics and Accountability for Innovation and Funding Initiatives.*** The Subcommittee recommends that DHS leadership direct more deliberate actions to measure progress on innovation and funding initiatives. Methods to measure progress could include, for example, the Department creating benchmarks for success of its innovation offices and then measure those offices against those benchmarks on an annual basis. In addition, the Department should consider conducting a survey of innovation industry partners in the same ways DHS is working towards surveying traditional customers on their experiences interacting with DHS.
5. ***Conduct an Internal Review of Contracting Authority and Processes for Mission-Supporting Technologies.*** While a comprehensive examination of procurement authorities and regulations was outside the scope of the Subcommittee’s review, the Subcommittee received information from relevant stakeholders throughout its brief review that the acquisition laws, regulations, and processes are at times difficult for components to navigate consistent with their intended goals of leveraging innovation from the private sector. The Secretary should direct that a review of the acquisition processes specifically related to procurement of new technologies that support operational activities across the Department be conducted to identify: i) processes that can be streamlined; ii) legal and regulatory requirements that can be clarified; and iii) legislative remedies that may be appropriate to seek from Congress, including the funding of an “innovation fund” that would provide seed funding for new projects.

CONCLUSION

Various components across DHS are working toward improving activities that leverage changing technologies in a way that supports departmental critical missions. Obtaining new technologies in a rapidly changing environment can be challenging to reconcile with extensive legal and regulatory frameworks and processes, but it is important the Department continue to modernize its efforts to do so. The Subcommittee has made five recommendations that, if implemented, can improve the Department’s management of its existing innovation efforts and interactions with private industry eager to engage with DHS, and spur greater collaboration and continuity across the DHS enterprise.

Secretary

U.S. Department of Homeland Security
Washington, DC 20528




**Homeland
Security**

October 16, 2022

MEMORANDUM FOR: William J. Bratton and Jamie Gorelick
Co-Chairs, Homeland Security Advisory Council

CC: Karen Tandy
Vice Chair, Homeland Security Advisory Council

FROM: Alejandro N. Mayorkas 
Secretary

SUBJECT: **New Homeland Security Advisory Council Subcommittees**

Thank you for your completed efforts on Disinformation Best Practices and Safeguards. I greatly appreciate the Subcommittee's and Council's thoughtful insights and recommendations, which we are implementing. I also appreciate the work the Customer Experience and Service Delivery Subcommittee has underway.

I now respectfully request that the HSAC form four new subcommittees to provide findings and recommendations in these critical areas of our work:

1. How the Department can take a greater leadership role in supply chain security, including by strengthening supply chain cybersecurity.
2. How the Department can improve upon its intelligence and information sharing with our key federal, state, local, tribal, territorial, and private sector partners. The subcommittee should assess whether the Department's information sharing architecture developed by the Office of Intelligence and Analysis (I&A) is adequate for the threats of today and tomorrow, and provide advice and recommendations to better enable I&A to rapidly and efficiently share information and intelligence with our key partners.
3. How the Department can improve its commitment to transparency and open government. The subcommittee should provide advice and recommendations that will position the Department as the leader in this critical area of model government conduct.

4. How the Department can create a more robust and efficient Homeland Security Technology and Innovation Network. The subcommittee should provide advice and recommendations that will develop the Department's innovation, research and development, and technology network with the private sector.

These subjects are described in more detail below. I will follow up with you shortly regarding formation of the subcommittees.

I request that the HSAC submit its findings and key recommendations to me no later than 120 days from the date of this memorandum, consistent with applicable rules and regulations.

Thank you for your work on these important matters, your service on the HSAC, and your dedication to securing our homeland.

Leadership in Supply Chain Security

The United States needs resilient, diverse, and secure supply chains to ensure our economic prosperity and national security. The Department of Homeland Security continues to protect America's national and economic security by facilitating legitimate trade and travel and rigorously enforcing U.S. customs and immigration laws and regulations.

Secure and resilient supply chains facilitate greater domestic production, a range of supply, built-in redundancies, adequate stockpiles, and a world-class American manufacturing base and workforce. Technology and stable and secure networks are critical to facilitating this work. In the current digital age, it is imperative that the U.S. not only manufacture key technologies like lithium-ion batteries and semiconductors, but also ensure that technology is in place to secure the supply chains of raw materials necessary to this manufacturing. The recently enacted "The CHIPS and Science Act of 2022" (CHIPS Act) made an historic investment in this space and makes ensuring the security of supply chains an even greater priority.

Eliminating forced labor from U.S. and global supply chains is a moral imperative and critical to ensuring global economic security. The Department serves as the Chair of the Forced Labor Enforcement Task Force (FLETF), which has taken a leading role in the implementation of the Uyghur Forced Labor Prevention Act (UFLPA). The UFLPA seeks to prohibit goods made with forced labor from the People's Republic of China (PRC) from being imported into the United States. The PRC's use of forced labor has weakened our national security posture, as well as that of our international partners, by systemically undercutting economic competitiveness in key sectors such as polysilicon and agriculture. The *FLETF's Strategy to Prevent the Importation of Goods Mined, Produced, or Manufactured with Forced Labor in the People's Republic of China*, presents a whole of government initiative to fight this scourge, and seeks stakeholder input to leverage partner capabilities.

Pandemics and other biological threats, cyberattacks, climate shocks and extreme weather events, and other conditions can reduce critical manufacturing capacity and the availability and integrity of critical goods and services. A resilient American supply chain will ensure domestic manufacturing capacity, maintain America's competitive edge in research and development, and

create well-paying jobs.

The Department and its components have already begun to make strides in this space. The Cybersecurity and Infrastructure Security Agency (CISA) has advanced work to increase supply chain security. The Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force – sponsored by CISA’s National Risk Management Center – is the United States’ preeminent public-private supply chain risk management partnership. The ICT SCRM Task Force identifies and develops consensus strategies that enhance supply chain security and resilience.

The U.S. Coast Guard’s Marine Transportation System Management mission enhances border security and defends the economic security of our \$5.4 trillion Marine Transportation System. This is in concert with the Maritime Security Operations mission program, which encompasses activities to protect waterways and ports by combating sea-based terrorism and other illegal activities.

The U.S. Customs and Border Protection (CBP) supply chain security mission is built on facilitation and layered enforcement. CBP’s Customs Trade Partnership Against Terrorism (CTPAT) works with the trade community to strengthen international supply chains and improve United States border security. CTPAT is a voluntary public-private sector partnership program that recognizes that CBP can provide the highest level of cargo security only through close cooperation with the principal stakeholders of the international supply chain such as importers, carriers, consolidators, licensed customs brokers, and manufacturers.

In addition to our work domestically, close cooperation on resilient supply chains with allies and partners who share our values will foster collective economic and national security. This request aligns with the DHS priority to maximize our international impact and strength, where we leverage our international footprint and relationships to advance homeland security objectives.

As the Department strives to stay ahead of the curve and take a greater leadership role by harnessing new technologies, minimizing environmental impact, and increasing partnerships in this vital area, I ask that you provide recommendations on how the Department can take a greater leadership role in supply chain security. The subcommittee’s assessment should include, but need not be limited to, the following:

- a. strengthening physical security;
- b. strengthening cybersecurity; and,
- c. increasing efficiencies to ensure a resilient, safe, and secure supply chain for critical manufacturing and technology sectors.

DHS Intelligence and Information Sharing

Federal, state, local, tribal, and territorial partners convened shortly after the September 11, 2001 terrorist attacks, creating a domestic information sharing architecture to enable the timely and seamless exchange of information to detect and eliminate terrorist threats. In the 21 years since 9/11, our law enforcement and homeland security community has made great progress in reshaping our information sharing environment. Working together, we put policies and processes in place that help us to be safer and more secure than we were years ago.

The Department of Homeland Security is committed to building on this foundation, as we are facing a more complex, diverse, and dynamic threat landscape than ever before. The wide array of threats we face impacts the safety and security of local communities of every size and location across our great country. The most effective way in which we address these challenges is through our partnerships, working together with one another.

DHS hosted an Intelligence Summit in August 2022, in partnership with the International Association of Chiefs of Police and other national law enforcement, public safety, and homeland security organizations. The Summit aimed to deepen partnerships and continue to improve intelligence and information sharing as public safety and national security threats evolve. The Summit also served as a forum to galvanize collaboration and commitment to supporting state, local, tribal, territorial, and campus (SLTTC) partners as they protect their communities. Senior leaders and key stakeholders convened with the goal of discovering new opportunities and improving existing avenues to enhance information sharing between all levels of government, while ensuring the protection of the privacy, civil rights, and civil liberties of U.S. citizens.

In June, DHS also launched a new mobile application titled DHS Intel, designed to deliver and share timely intelligence information with law enforcement and first responders across the country. Today, many of us consume information from news feeds, blogs, social media, podcasts, and a variety of other sources on our mobile phones; however, until last month, most intelligence information was either sent via e-mail distribution lists or viewed on sites optimized for desktops and laptops. Now, this information is available on-the-go for SLTTC and federal partners who rely on intelligence to keep the country safe.

As the Department approaches its 20th Anniversary, I ask that you provide recommendations on:

1. How the Department can rapidly and efficiently share intelligence and information with its federal, state, local, tribal, territorial, and private sector partners. Have DHS investments in information sharing technology and changes in law and policy resulted in increased knowledge transfer and resilience? Are further investments or changes in law or policy needed?
2. Has DHS created an information and intelligence sharing architecture that efficiently spreads knowledge and rapidly shares critical information? Are there steps that we need to take to revitalize or improve this architecture?

3. Whether the current DHS information sharing architecture optimizes information sharing for threats other than counterterrorism; for example, cyber, border security, foreign influence/propaganda, strategic advantage, and others.
4. Internal DHS Information Sharing: Has DHS fully implemented internal DHS information sharing policy – for example, the One DHS Memo – to leverage DHS data and information to support Departmental missions like border security as well as to develop and share relevant, quality intelligence with our partners?

DHS Transparency and Open Government

DHS is committed to transparency and promoting the principles of an Open Government. Initially developed in 2009 under the Obama Administration, the Presidential Memo on Transparency in Government and the follow-on Open Government Directive from the Office of Management and Budget laid a road map for increasing openness and transparency.

The United States has worked both domestically and internationally to ensure global support for Open Government principles to promote transparency, fight corruption, energize civic engagement, and leverage new technologies in order to strengthen the foundations of freedom in our own nation and abroad.

DHS has expanded transparency in concert with the development of Open Government Plans, recognizing that increased access to research data and information can encourage research collaboration and help successfully address the nation's constantly evolving homeland security challenges.

Further, I identified increasing openness and transparency as a key priority for our Department. It is important that DHS build and maintain trust with the communities we serve through improved data transparency, robust external communication, and strengthened oversight and disciplinary systems.

Therefore, I ask that you provide recommendations on:

1. How the Department and its components can expand on the foundation set by previous Open Government Plans for DHS.
2. New initiatives to increase transparency and sustaining its mission to protect the homeland.
3. How DHS can be held accountable in meeting its commitment to be a leader in modeling government openness and transparency.

Homeland Security Technology and Innovation Network

The Department of Homeland Security employs more than 240,000 individuals working in multiple offices and components across the country and the world. While the mission is uniform across the Department – to protect the homeland from foreign and domestic threats

– the tools necessary to accomplish this can vary widely by office and can change in time. Moreover, while some threats are known and have been core to the DHS mission since our inception, we must remain ever vigilant and responsive to countering both unknown and future threats. In this scenario we may face accelerated timelines that do not fit into our normal acquisition life cycle to acquire key technology to counter a threat. It is critical to our nation’s security to have a robust and efficient Homeland Security Technology and Innovation Network that promotes an enhanced schedule of development and deployment of critical technology and assets to protect the homeland.

Such a network will necessarily require deep partnerships, especially with the private sector. From enterprise software to digital driver’s licenses, private sector entities have enabled the Department to advance its mission and modernize. It is therefore important for the Department to leverage its existing offices and relationships to further harness the potential of technology and innovation in the private sector to benefit the Department.

Current technology and innovation engagements are led by the DHS Science and Technology Directorate (S&T) and designated offices within component agencies. S&T is responsible for identifying operational gaps and conceptualizing art-of-the-possible solutions that improve the security and resilience of the nation. To facilitate this, S&T oversees programs that facilitate technology transfer and commercialization, funding for start-ups, research, and development challenges. Similarly, component offices partner with private sector entities to source technology and innovations for their discrete needs.

To maximize the opportunity afforded by partnership with the private sector and the expertise within the Department, I ask that you assess the private sector experience, specifically in the areas of technology development and innovation, and provide recommendations on how the Department can create a more robust and efficient Homeland Security Technology and Innovation Network.

The subcommittee’s assessment should include, but need not be limited to, the following:

- a. an assessment of how the private sector engages with the current R&D and acquisition programs and opportunities, including where those can be maximized or improved;
- b. different means of increasing innovative technology partnerships with the private sector;
- c. recommendations on harmonizing existing innovation efforts across the Department and its components to best leverage funding and resources; and,
- d. identifying current barriers to developing a more robust technology and innovation network, including legal, contracting, and policy considerations.

APPENDIX 2: SUBJECT MATTER EXPERTS AND OTHER WITNESSES

<u>Name</u>	<u>Title</u>	<u>Organization</u>
Melanie Alston	Deputy Head of Contracting Activity	Immigration and Customs Enforcement
Julie Brewer	Executive Director	Innovation and Collaboration, DHS Science & Technology
Melissa Conley	Acting Deputy Administrator	TSA Requirements and Capabilities Analysis
Daniel Cotter	Director	First Responders Group, DHS Science & Technology
Kathryn Coulter	Chief of Staff	DHS Science & Technology
Anil Dewan	Senior Advisor	DHS Office of Chief Information Officer
Deborah Fleischaker	Acting Chief of Staff	Immigration and Customs Enforcement
CDR Rebecca Fosha	Acting Office Chief	Office of Research Development, Test and Evaluation (CG-926), U.S. Coast Guard
James Gilkeson	Director	TSA, Innovation Task Force
Andrew Haskins	Deputy Chief Innovation Officer	Transportation Security Administration
Rachelle Henderson	Chief Information Officer	Immigration and Customs Enforcement
James Johnson	Principal Director	Office of Science and Engineering
Michel Kareis	First Responders Group	DHS Science & Technology
CAPT Daniel Keane	Commanding Officer	Research and Development Center, U.S. Coast Guard
Meg King	Executive Director	TSA Office of Strategy
Dimitri Kusnezov	Under Secretary	DHS Science & Technology
David Larrimore	Chief Technology Officer	Office of Chief Information Officer
Jamie Lawrence	Deputy Assistant Secretary	Private Sector Office

Megan Mahle	Division Director	DHS Science & Technology
Jonathan Mcentee	Operations and Requirements Analysis Director	DHS Science & Technology
Christopher Moman	Assistant Director / Component Acquisition Executive	Immigration and Customs Enforcement
Angela Noyes	Office of Chief of Staff	DHS Science & Technology
Jeremy Ocheltree	Director	CBP Innovation Team
Steven Parker	Chief Innovation Officer	Transportation Security Administration
Joshua Powell	Deputy Director	CBP Innovation Team
Krista Powers	Vice President	Client Success, IDEMIA Identity and Security
Michael Robertson	Senior Advisor	DHS Science & Technology
Michael Steckman	Chief Revenue Officer	Anduril
Lisa Sullivan	Executive Vice President	Travel and Transport, IDEMIA Identity and Security
Alexandra Swan	Strategic Planner	Office of Research Development, Test and Evaluation (CG-926), U.S. Coast Guard
Benjamin Teed	Unit Chief	HSI Innovation Lab, ICE

APPENDIX 3: DHS INNOVATION OFFICES

DHS Component/Directorate	Innovation Program Office
U.S. Citizenship and Immigration Services (USCIS)	Innovations in Citizenship Education Program
U.S. Coast Guard (USCG)	Acquisition Directorate Office of Research, Development, Test, Evaluation, and Innovation (RDT&E) and Innovation Program
U.S. Customs and Border Protection (CBP)	The Innovation Team (INVNT)
Cybersecurity and Infrastructure Security Agency (CISA)	Cyber Innovation Fellows Initiative
Federal Emergency Management Agency (FEMA)	Office of National Continuity Programs
Federal Law Enforcement Training Center (FLETC)	Training Innovation Division (TID)
U.S. Immigration and Customs Enforcement (ICE)	Office of the Chief Innovation Officer (ICE OCIO) HSI Innovation Lab powered by The Repository for Analytics in a Virtualized Environment (RAVEN)
U.S. Secret Service (USSS)	USSS Office of Enterprise Readiness (ERO) USSS Office of Strategic Planning & Policy (OSP) Emerging Capabilities Division (ECA)
Management Directorate	DHS Procurement Innovation Lab (PIL) Office of the Chief Procurement Officer
Transportation Security Administration (TSA)	Innovation Task Force (ITF)
Science & Technology Directorate (S&T)	Office of Innovation and Collaboration Office of Mission and Capability Support Office of Science and Engineering Federally Funded Research and Development <ul style="list-style-type: none"> • Homeland Security Operational Analysis Center (HSOAC) • Homeland Security Systems Engineering and Development Institute (HSSEDI)