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.