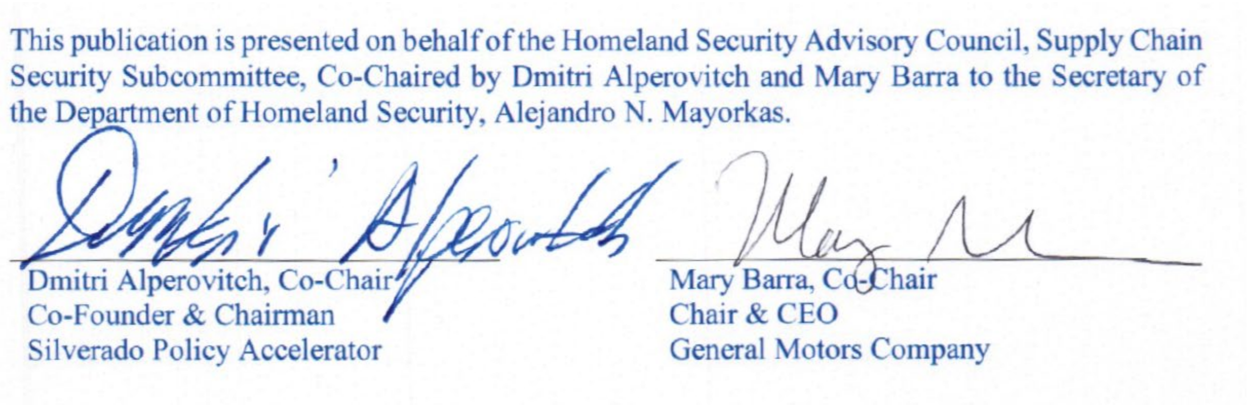
Homeland Security Advisory Council

Supply Chain Security Subcommittee

Final Report

March 16, 2023



This publication is presented on behalf of the Homeland Security Advisory Council, Supply Chain Security Subcommittee, Co-Chaired by Dmitri Alperovitch and Mary Barra to the Secretary of the Department of Homeland Security, Alejandro N. Mayorkas.

Dmitri Alperovitch, Co-Chair
Co-Founder & Chairman
Silverado Policy Accelerator

Mary Barra, Co-Chair
Chair & CEO
General Motors Company

This page is intentionally left blank.

TABLE OF CONTENTS

SUBCOMMITTEE FOR SUPPLY CHAIN SECURITY

Dmitri Alperovitch, Co-Chair	**Co-Founder and Chairman** **Silverado Policy Accelerator**
Mary Barra, Co-Chair	**Chair and Chief Executive Officer** **General Motors Company**
Dr. Tarika Barrett	**Chief Executive Officer** **Girls Who Code**
Jane Harman	**Distinguished Fellow and President Emerita** **The Woodrow Wilson Center**
Elizabeth Shuler	**President** **American Federation of Labor and Congress of Industrial Organizations**
Candace Archer	**Policy Director** **American Federation of Labor and Congress of Industrial Organizations**
Craig Glidden	**Executive Vice President of Global Public Policy** **General Motors**
Sarah Stewart	**Chief Executive Officer and Executive Director** **Silverado Policy Accelerator**

HOMELAND SECURITY ADVISORY COUNCIL STAFF

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

EXECUTIVE SUMMARY

This Subcommittee for Supply Chain Security ("Subcommittee") was tasked by the Secretary of Homeland Security to look at what steps the Department can take to enhance the security, resiliency, and efficiency of the nation's supply chains. The Department of Homeland Security protects America's national and economic security by facilitating legitimate trade and travel and rigorously enforcing U.S. customs and immigration laws, as well as sanctions, export controls, and other vital national security regulations.

Since November 2022, the Subcommittee met with leaders and subject matter experts from the Department and private sector entities. The briefings underscored the vital and central role that the Department plays in the nation's supply chain and have been essential to help the Subcommittee identify room for improvement and better coordination across the Department.

This report presents the **ten** specific recommendations that the Subcommittee believes can help DHS improve the resiliency and security of the nation's supply chain and overall national security. The recommendations are in two categories aimed to prioritize supply chain resilience and efficiency.

Augment and Prioritize Supply Chain Resiliency Tools and Resources

1. Explore creation of a Supply Chain Resiliency Center (SCRC).
2. Revise and expand Section 9 list of critical infrastructure entities maintained by CISA.
3. Seek additional legislative authorities for Component programs.
4. Improve sharing of classified threat information by CISA with Section 9 list entities and other critical private sector partners.

Enhance Efficiency and Security of Screening of Imports and Exports

5. Improve information sharing and operational efficiencies across the Department.
6. Increase interagency cooperation between DHS, Department of Commerce and Department of Treasury to enhance efforts to enforce the nation's export controls and sanctions.
7. Increase customs cooperation with allies and key partners to enhance information sharing and enforcement.
8. Improve utilization of CBP resources and personnel.
9. Bolster Customs Trade Partnership Against Terrorism (CTPAT) enrollment.
10. Assess efficacy of TWIC card program use at national ports.

The Subcommittee's report outlines our methodology, key findings, and recommendations that fortify the Department's authorities, frameworks, and resources.

METHODOLOGY

The Subcommittee drew upon expert interviews and supplemental research from November 2022 to February 2023. In particular, the subcommittee met with representatives, subject matter experts and leaders from the DHS Office of Strategy, Policy, and Plans (PLCY), U.S. Customs and Border Protection (CBP), Cybersecurity and Infrastructure Security Agency (CISA), U.S. Immigration and Customs Enforcement (ICE), and Homeland Security Investigations (HSI). These briefings were valuable and provided background information to inform our recommendations.

The Subcommittee also conducted a multisite visit in Los Angeles to meet with CBP, Transportation Security Agency (TSA), United States Coast Guard (USCG), private industry, and The Port of Los Angeles (POLA). The Subcommittee toured facilities for a firsthand look at seaport and air cargo screening operations. The Subcommittee was able to receive briefings and tours from the primary DHS components that work to ensure a secure supply chain every day. The Subcommittee wants to take this opportunity to thank all of the individuals whom we met while there. The trip to Los Angeles was very insightful and helped shape some of our recommendations.

The overall methodology was to focus on key areas that could make an immediate impact and increase DHS leadership in supply chain security and resiliency. The Subcommittee recognizes that DHS alone, or even the U.S. Government as a whole, does not control the supply chain but can have influence and can impact the supply chain in many ways.

KEY FINDINGS

The Subcommittee has determined that the Department plays a vital role in the nation's supply chain, including in the processing and screening of imports and exports coming into and out of the country.

The Subcommittee identified a number of improvements and efficiencies that could be made to security screening of imports coming into the country, as well as enhancements to the screening and enforcement of export control and sanctions policies for exports.

The Subcommittee has also determined that the Department could expand its role in identifying critical supply chain gaps that could present significant economic or national security risks, including using the Defense Production Act (DPA) and other authorities foster collaboration and help secure, manufacture, prioritize, or facilitate importation of vital components needed by the U.S. private sector in anticipation of supply chain disruptions.

A key overlay to all these recommendations is a worker-centric focus. Supply chain security has benefitted from technical advances, but the briefings reinforced the importance of trained officers and workers as essential to mission success, particularly when technology fails. Establishing a secure supply chain depends on understanding the experiences of frontline workers since their daily interactions with processes and technology can highlight gaps in our understanding of where security threats may exist. Ensuring the participation of workers as full partners should be understood to accompany the implementation of the following recommendations.

RECOMMENDATIONS

The recommendations of the Subcommittee for Supply Chain Security fall into two general categories: recommendations for enhancing Supply Chain resiliency and efficiency and security of screening of Imports and Exports.

1. Augment and Prioritize Supply Chain Resiliency Tools and Resources

(a) *Explore Creation of a Supply Chain Resiliency Center (SCRC)*

The Subcommittee recommends that the Department explore the feasibility of establishing a Supply Chain Resiliency Center (SCRC) within the Department's Office of Strategy, Policy, and Plans. The SCRC could aggregate and disseminate information across the Department, as well as the broader U.S. government and private sector, about critical supply chain vulnerabilities and disruptions that can have a disproportionate negative effect on the U.S. economy, the livelihood of American citizens, or protection and continuity of U.S. critical infrastructure. The SCRC could also facilitate the development of inter-governmental and public-private solutions to such challenges. The Department should assess which component agencies should provide personnel, expertise, and resources to the SCRC to help in the conduct of its mission.

The Subcommittee appreciates that realizing the full vision of SCRC will take time and resources and recommends to the Secretary to request appropriate funding from Congress for this new mission priority. The Subcommittee recommends that even in the absence of a SCRC, the Department should look to prioritize implementation of the recommendations herein with an eye towards future SCRC creation. Specific ways the SCRC or equivalent can advance supply chain resiliency include but are not limited to:

- Use of DPA and other authorities to foster collaboration and prioritize or even guarantee domestic manufacturing of needed critical goods in response to a supply chain disruption, as well as in anticipation of one;
- Mapping of existing supplies, demand projections and chokepoints for critical goods to determine a strategy for preventing and mitigating a supply chain disruption or crisis, including for example, stockpiling critical goods and instituting an early warning system for disruptions where information is disseminated early to other government agencies and private sector entities;
- Signing of bilateral supply chain security agreements with allied and partner countries to acquire goods and resources necessary to keep critical U.S. industries operating in times of crisis;
- Working with USCG, CBP and TSA, as well as ports and airports, to prioritize unloading and secure screening of inbound cargo that contains such vital resources; and
- Developing an appropriate system for seeking input from frontline employees and their unions.

Here are some examples of how SCRC, if it had existed, might have helped to address major supply-chain related economic disruptions of recent times:

- During last year's unprecedented container ship backlog at the ports of LA/Long Beach, such a Center could have conducted a review of the root causes of the problem and recommended solutions to the Department.
- During the recent chips and baby formula shortages, SCRC could have worked with other DHS agencies to prioritize rapid but safe processing of such imports already in queue to be unloaded into the United States.
- SCRC could have also worked with international allies and partners to get priority allocations of needed resources for U.S. industry or worked with the inter-agency to invoke DPA with the relevant private sector entities to increase manufacturing capacity of necessary supplies at home.

i. Conduct an After-Action Report on Supply Chain Challenges and Shipping Backlogs of 2021-2022

During its site visits to the ports of LA/Long Beach, as well as the LAX cargo screening facility, the Subcommittee heard a range of views and rationales for the causes of the disruption. It became clear to us that no authoritative root cause analysis has been done on one of the major supply chain issues impacting the U.S. economy and contributing to the rise of inflation in recent years. A comprehensive After-Action Report could identify crucial improvements that could be made to reduce the impact of future backlogs. The report could be prepared by the SCRC, if established. The report should be wide-ranging in its information gathering in order to take into account as many explanations for the disruption as possible when developing recommendations for how DHS component agencies could enhance information sharing, communication and coordination with the White House, Department of Commerce, and other relevant agencies to address future supply chain disruptions.

ii. Develop Tabletop Exercises with Key Stakeholders

The Subcommittee recommends that SCRC or equivalent work with CISA to develop tabletop exercises with the key stakeholders in the supply chain, such as private sector companies, workers and their unions, to model the impact of both cyber-related and other supply chain disruptions on the ability of the nation's logistics infrastructure to import and export goods.

(b) ***Revise and Expand Section 9 List of Critical Infrastructure Entities maintained by CISA***

CISA currently maintains a list of critical infrastructure entities that meet the criteria specified in Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, Section 9(a) ("Section 9 entities") of private sector critical infrastructure entities "where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security."[1] This list is very helpful in determining which companies are vital to the U.S. economy from a cybersecurity resilience perspective. However, its value can be substantially increased, if other critical economic industries are included even if they do not face a substantial cybersecurity threat. The Subcommittee recommends revising the Section 9 List to include all substantial private sector entities, which if they were to suffer an IT-related, physical, or supply chain disruption, would have a large and disproportionate impact on the U.S. economy and national security.

(c) ***Seek Additional Legislative Authorities for Component Programs***

The Subcommittee recommends that the Department work with Congress to restore administrative subpoena power for Homeland Security Investigations (HSI) and Customs and Border Protection (CBP) to enhance their ability to conduct Export Control violation investigations. Such subpoena authority (previously authorized in 50 U.S.C. § 4614(a)(1)) was left out of the Export Control Reform Act of 2018 (ECRA). This subpoena was utilized by HSI and CBP to request from individuals and entities export records pertaining to attempted export of dual-use items. The Subcommittee learned that it was a powerful tool for the respective agencies, as it would allow CBP Officers and HSI Special Agents to determine if an export criminal violation existed in a timely manner. Since cargo rarely stays in one location long, a timely lawful process to receive such critical information for export enforcement is essential for preventing prohibited items from being exported from the United States. The Subcommittee has heard from agencies that the loss of this administrative subpoena has hindered export enforcement investigations and potentially allowed prohibited items to be illegally exported from the country.

The Subcommittee also recommends that the Department work with Congress on administrative

[1] Federal Register :: Improving Critical Infrastructure Cybersecurity

Subpoena Power for CISA to receive relevant proprietary and confidential economic information necessary for determining eligibility of companies for expanded Section 9 List inclusion. Like the subpoena authorities that the International Trade Commission (ITC) uses to securely and confidentially aggregate private sector economic data to advise the Executive and Legislative Branches on international trade issues, CISA could use similar authority to put together an accurate and comprehensive but secure and confidential list of U.S. critical economic infrastructure entities.

(d) ***Improve sharing of classified threat information by CISA with Section 9 list entities and other critical private sector partners***

The Subcommittee recommends that CISA explore ways to grant more clearances to vetted critical private sector partners. It also recommends that CISA partner with other departments and agencies such as HSI and FBI, to get temporary access to their Sensitive Compartmented Information Facilities (SCIFs) around the country to remotely brief their cleared private sector partners.

The Subcommittee heard from CISA that briefing classified threat information to relevant private sector partners in a timely manner remains a significant challenge, both in part due to lack of sufficient number of cleared personnel at such companies, as well as due to their physical distance from a CISA SCIF. While we believe that more efforts should be made to encourage declassification of relevant information for its wider dissemination, we recognize that this is not always possible, or is at the control of CISA, due to it rarely being the original classification authority. Thus, we believe it is important to prioritize clearing more private sector personnel and developing options to temporarily use the secure space of other agencies, when the need arises, to conduct secure briefings for relevant parties.

In addition, the Department should strive to declassify as much threat information as feasible with its counterparts across the Intelligence Community in order to make it as broadly available as possible.

2. Enhance Efficiency and Security of Screening of Imports and Exports

(a) ***Improve Information Sharing and Operational Efficiencies Across Department Components with Shared or Similar Missions***

The Subcommittee found that CBP officers are highly effective at identifying potentially problematic inbound and outbound cargo flows due to the use of its Automated Targeting System (ATS). We recommend that relevant TSA, HSI and USCG officers get the maximum access possible to ATS data, as well as shipping manifests, in order to better fulfill their separate security and investigative missions.

The Subcommittee determined that significant efficiencies and security enhancements can be gained by resolving duplication of effort in screening of inbound and outbound cargo by CBP, TSA and USCG personnel, as well co-locating officers from different agencies in places where it makes sense.

For example, the Subcommittee was very impressed by TSA's use of state-of-the-art private sector facilities to perform comprehensive screening of all outbound air cargo for explosives and other threats to civilian aviation. The Subcommittee believes that CBP would benefit greatly at co-locating their personnel at such facilities to screen that same cargo for other prohibited items of concern to them, rather than operate separate screening operations elsewhere. Such colocations could not only result in a higher rate of screened outbound air cargo by CBP and reduce costs, but also speed up the export of legitimate cargo to facilitate commerce.

The Subcommittee also discovered that inbound shipping containers are checked separately by CBP and USCG, as both agencies have missions to look for different issues: USCG focusing primarily on safety violations, while CBP looking for import and other criminal law violations. The Subcommittee believes further efficiencies and higher rate of screening can be achieved if CBP and USCG officers work jointly together in the examination of containers for their relevant missions.

A comprehensive review of how CBP, TSA and USCG screen inbound and outbound cargo at their various facilities could identify other similar possibilities for improved efficiency and Department cohesion.

(b) ***Increase interagency cooperation between DHS, Department of Commerce and Department of Treasury to enhance efforts to enforce the nation's export controls and sanctions***

i. Increase Coordination between HSI and Bureau of Industry and Security (BIS) at the Department of Commerce.

The Subcommittee found that cooperation between the two agencies vital to enforcing our export controls and must be a top priority. The Subcommittee recommends that the heads of both agencies develop a plan for enhancing their coordination, fully share access to relevant data sources and collaborate better in investigations.

ii. Promulgate new regulations requiring advanced electronic data collection from carriers in relation to exports, similar to the "24 hour rule" requirement that CBP has for importers to provide detailed manifest data 24 hours prior to loading cargo on a ship or airplane.

The Subcommittee heard from CBP officers that acquiring such manifest data in advance of export shipments would be of significant assistance to them in their mission to stop prohibited exports from leaving the country. Section 343 of the Trade Act of 2002 (19 U.S.C. Section 1415) provides legal authority for CBP to pass regulations requiring carriers to provide advance electronic manifests in all modes of transportations.

(c) ***Increase customs cooperation with allies and key partners to enhance information sharing and enforcement***

Customs Mutual Assistance Agreements (CMAAs) can be an important tool among allies and key trading partners to improve information exchange that can aid in enforcement efforts by having multiple authorities working in concert to intercept illicit goods in transit across borders. CMAAs can also be used to help expedite the flow of legal goods and avoid supply chain disruptions.

The Subcommittee recommends an assessment of existing CMAAs and how they can be further enhanced, as well as which countries may be priority candidates for new CMAAs.

(d) ***Improve Utilization of CBP Resources and Personnel***

i. Fully inventory seized cargo only when it is important and utilize technology to do so

The Subcommittee was briefed on how a considerable portion of CBP officers' time is used on the inventorying seized goods after their discovery. At the ports of LA and Long Beach, much of these goods consist of counterfeit fashion items that present no national security risk and the inventorying of which does not enhance the security of the country. By limiting the types of goods that need to be fully inventoried and utilizing digital inventorying technology to do so, CBP officers can spend more of their time on screening cargo for threats. The Department should look at legal and prosecutorial considerations in changing this policy.

ii. Use environmentally friendly disposal methods for seized cargo

The Subcommittee discovered that at the port of LA and Long Beach, most of the seized cargo goes through an incinerator. We recommend that CBP explore ways to sell some of the confiscated items (in their original or deconstructed form), particularly counterfeit goods, to recyclers in order to dispose of them in an environmentally safe way, as well as potentially save taxpayer funds.

iii. Increase Forward Deployment Abroad

The Subcommittee notes the importance and potential efficiencies of inspecting goods prior to reaching the ports and recommends that the Department enhance these efforts.

iv. Explore Policy Changes and Digitization to Optimize Inspection

The Subcommittee heard that during an inspection, if counterfeit goods are discovered the entire container must be searched even if the counterfeit product does not pose an immediate threat to national security or human health. To optimize finite inspection resources, the subcommittee recommends a policy change that, in the event counterfeit goods are discovered in whatever form in a shipping container, CBP would presume the entire container is counterfeit and stop the search. The burden would then shift to the importer to refute the presumption. The Subcommittee also recommends that all inspections that uncover counterfeit goods are entered into a searchable database that can be a further tool to aiding with targeting and risk-based inspections.

(e) ***Bolster Customs Trade Partnership Against Terrorism (CTPAT) Enrollment***

CTPAT is a critically important CBP private sector partnership program to voluntarily enroll importers who are willing to work with the agency to implement specific security measures, identify security gaps and assist CBP in its mission of assuring that the cargo coming into the United States is safe and legal. Currently over 50% of inbound cargo coming into the U.S. is by a CTPAT importer, which means that CBP has to use fewer resources to do the labor-intensive work of screening these containers.

The Subcommittee recommends that CBP examine what it would take to encourage more private sector importers to sign onto the program, without compromising its strict security vetting requirements. Substantially raising the percent of inbound cargo that comes into the country by a CTPAT importer would make the nation safer, free up more CBP resources to focus on screening non-CTPAT cargo and speed up the processing of inbound shipments through the nation's ports of entry.

(f) ***Assess efficacy of TWIC card program use at national ports***

During its port visit, the Subcommittee found inconsistent checking of TWIC cards that may undermine the security of maritime facilities that the program was designed to bolster. The Subcommittee recommends that TSA perform a comprehensive evaluation of the TWIC program that incorporates the experiences of terminal operators and frontline employees and their unions who are required to have this credential. A comprehensive review would assess the challenges and impediments that terminal operators, truck drivers, longshoremen, mariners, port employees, and other relevant parties face in applying for, renewing, using or checking the credential at relevant ingress and egress points into our national ports and determine solutions for addressing them.

CONCLUSION

The Department has a critical mission to secure the nation from a range of threats to our homeland and national security, including by enhancing the security, resiliency, and efficiency of the nation's supply chains, and facilitating legitimate inbound and outbound trade. In the wake of the COVID-19 pandemic and supply chain disruptions, the Department has made significant progress assessing continuing threats and implementing new measures to protect and strengthen supply chains and enforce U.S. trade laws. These threats will only grow and adapt, and the Subcommittee has outlined recommendations herein to further strengthen the Department's authorities, frameworks, and resources in a way that is durable as well as proactive, with benefits for our government, businesses, and workers.

APPENDIX 1: TASKING LETTER

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

Name	**Title**	**Organization**
Lazaro Alvarez	Transportation Security Inspector	TSA LAX Field Office
Emlyn Arrocha	Director, Global Product Compliance	Expeditors International
John Beckius	Executive Director	TSA Cargo Division, Policy, Plans and Engagement
Larry Betts	Facilities Manager	Expeditors International
Ian Brown	Chief	Risk Management Coordination, National Risk Management Center (NRMC), CISA
CDR Stephen Bor	Commander	LA/LB USCG
Chris Chase	Cargo Marketing Manager	Port of Los Angeles (POLA)
MST1 Adrian Camacho	Marine Science Technician	LA/LB USCG
John Paul Delgado	Unit Chief	Counter-Proliferation Investigations Unit, HSI, ICE
Mike DiBernardo	Deputy Executive Director for Marketing and Customer Relations	Port of Los Angeles (POLA)

Michael Duretto	Acting Deputy Federal Security	TSA
Eric Falcon	Senior Advisor to the Under Secretary for Policy	Office of Strategy, Policy, and Plans
Manuel Garza	Director	Customs Trade Partnership Against Terrorism (CTPAT), CBP
Chief Thomas E. Gazsi	Deputy Executive Director, Chief of Public Safety and Emergency Management	Port of Los Angeles (POLA)
Francisca Goncz	District Trade Compliance	Expeditors International
MSTC John Herman	Marine Science Technician	
LT David Hetticher	Lieutenant	LA/LB USCG
Tasha Hippolyte	Deputy Assistant Secretary	Office of Strategy, Policy, and Plans
John Houck	TSA Surface Inspector	TSA
Tung Huynh	Stakeholder Manager	TSA
Scott Jarrell	Chief of Staff	U.S. Customs and Border Protection (CBP)
Rich Koike	Section Chief	U.S. Customs and Border Protection (CBP)

Donald Kusser	Port Director	U.S. Customs and Border Protection (CBP)
Jim Lambropoulos	Deputy Assistant Administrator	TSA OSO/HQ Compliance
David Lampner	Supervisory Transportation Security Inspector	TSA LAX Field Office
Jamie Lawrence	Deputy Assistant Secretary	Private Sector Office
MST2 Noah Lighthart	Marine Science Technician	LA/LB USCG
Shon Lyublanovits	C-SCRM PMO Lead	Cybersecurity Division, CISA
John Pickle, Jr.	Principal Director	Trade and Economic Competitiveness, Office of Strategy, Policy, and Plans
CDR Tim McNamara	Commander	LA/LB USCG
CAPT Ryan Manning	Captain	LA/LB USCG
Jose Molina	Regional Vice President USA, Southwest	Expeditors International
Eric Mooney	LAX Branch Manager	Expeditors International
Thomas Overacker	Director	National Targeting Center – Cargo Division, CBP

Jason Pantages	Federal Security Director	TSA
Steve Pasienski	District Compliance Manager	Expeditors International
Jim Platt	Associate Director (A)	Planning & Coordination Division, National Risk Management Center (NRMC), CISA
Armando J. Quesada	Assistant Federal Security Director Inspections/Compliance	TSA
Roberto Romero	Warehouse Manager, FSC	Expeditors International
Michael Rose	Unit Chief	National Intellectual Property Rights Coordination Center, HSI, ICE
Carlton Ruesch	LAX District Manager	Expeditors International
Gene Seroka	Executive Director	Port of Los Angeles (POLA)
Robert Silvers	Under Secretary	Office of Strategy, Policy, and Plans
Amy Spell	FASC Program Lead	Cybersecurity Division, CISA
Sheeva Varughese	Chief Technology Officer	Port of Los Angeles (POLA)
Tirza Verduzco	Transportation Security Inspector	TSA LAX Field Office

Katherine Willers	Initiative Manager for Supply Chain Risk Management	National Risk Management Center (NRMC), CISA
Dennis Wilson	Section Chief	U.S. Customs and Border Protection (CBP)
Tony Zhong	Chief Information Security Officer	Port of Los Angeles (POLA)