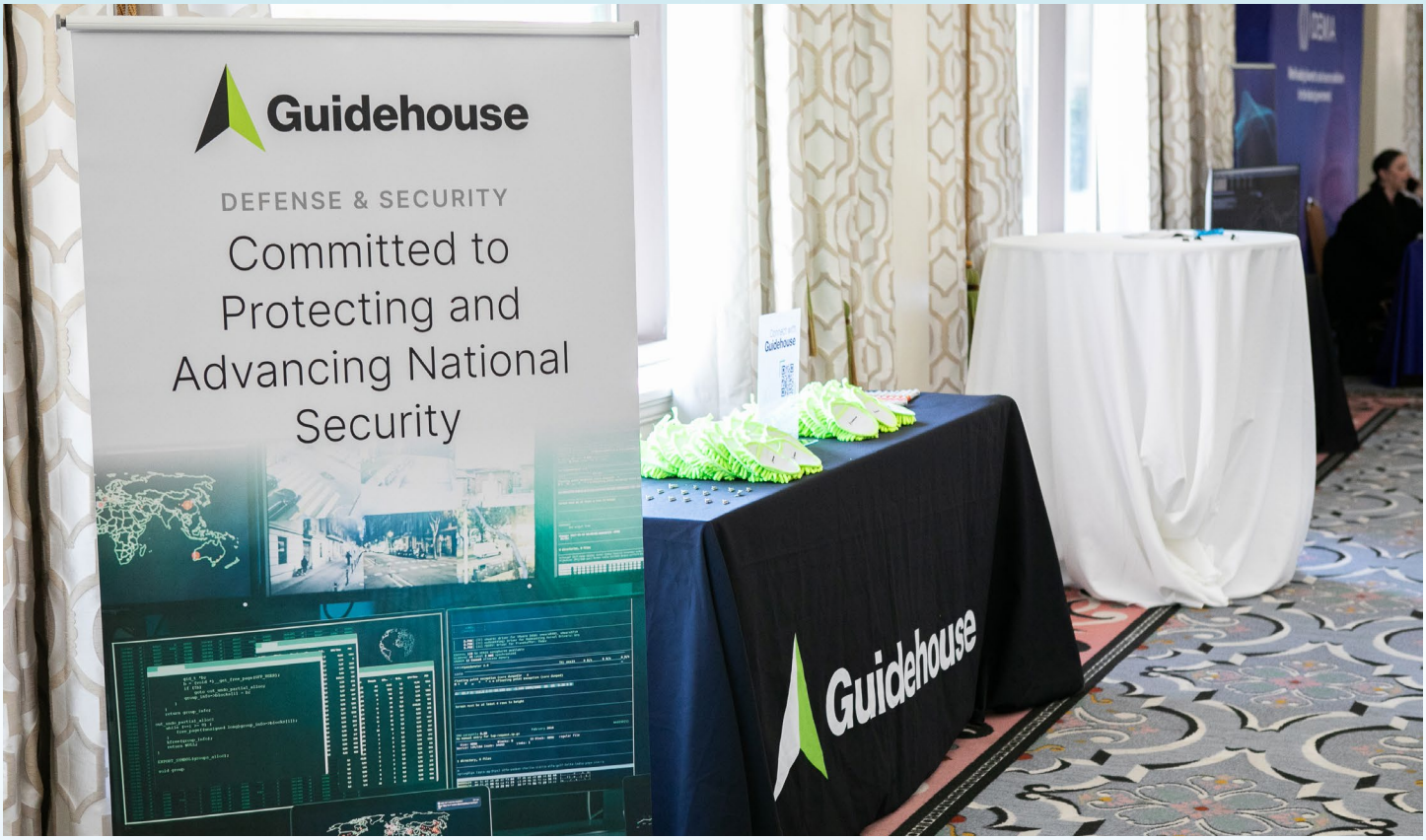
SESSION RECOMMENDATIONS

ADVANCING THE ENTERPRISE

PRESENTED BY

Guidehouse
outwit complexity™

THANK YOU



Guidehouse
outwit complexity™

This report was prepared by Guidehouse. We would like to acknowledge:

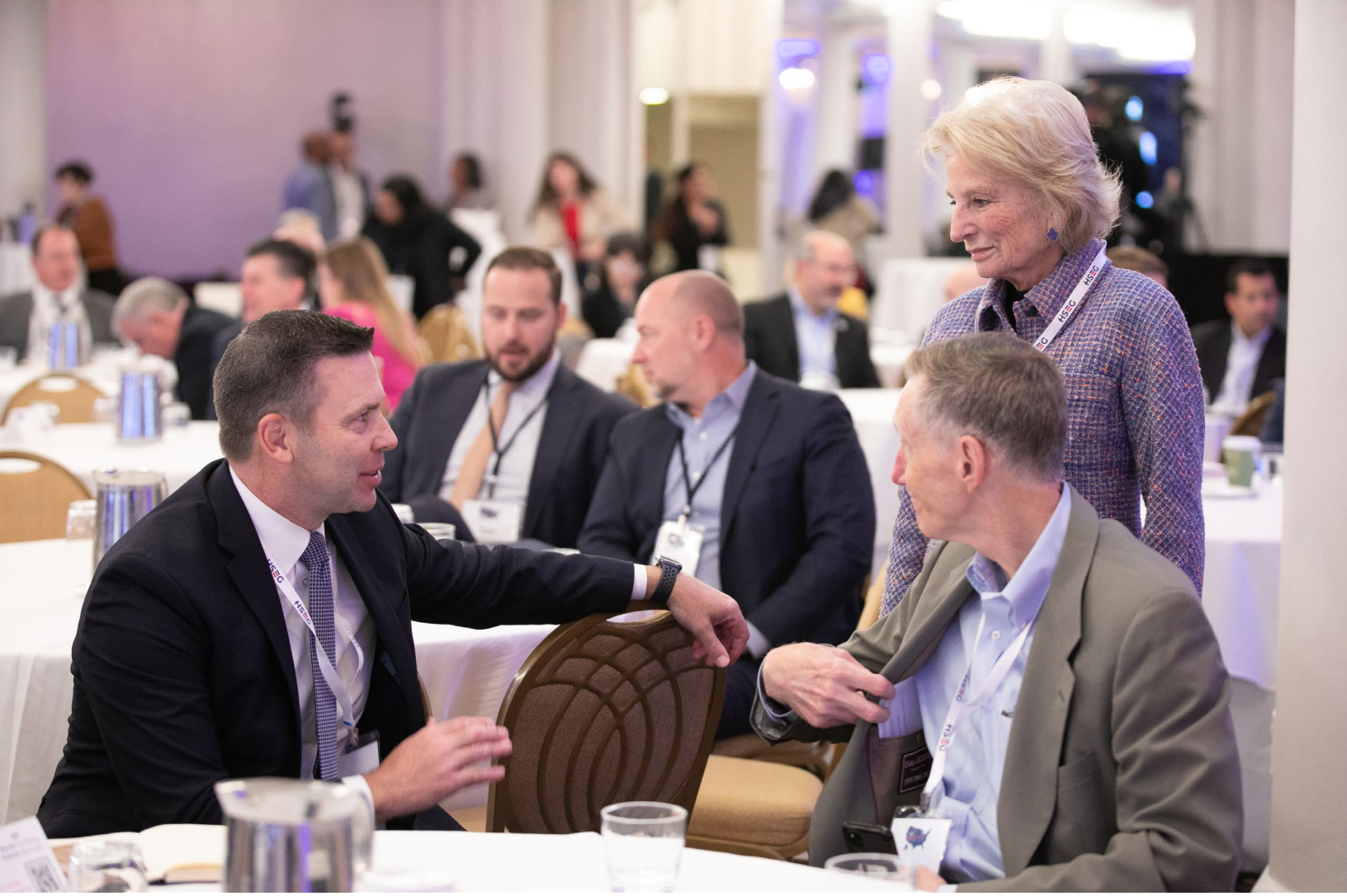
Notetakers:

Sahar Amini | Aliza Asad | Ben Gorban | Donald Ross
Kristyn Shapiro | Isabelle Solomon

Authors:

Patricia Cogswell | Kristyn Shapiro | Ben Gorban | Isabelle Solomon

www.guidehouse.com



INTRODUCTION

Collaboration, Partnership, Whole of Nation Approach. Evolution of the Threat. Improving Customer Experience. Enhancing Efficiency and Effectiveness. Mitigating Risk and Increasing Resilience of the Elements Critical to our Economic Security. The 2023 Homeland Security Enterprise Forum (HSEF) explored these core elements as part of its overarching theme—Advancing the Homeland Security Enterprise.

The Hamas attacks on Israel that killed more than 1,300 civilians on October 7, 2023, two days before the 2023 HSEF, factored into many of the HSEF session discussions. It served as a stark reminder to all that homeland security is as much an imperative today as when the Department of Homeland Security (DHS) was created in 2003.

Over a two-day event, subject matter experts from government, academia, industry, and the private sector contributed to an in-depth discussion about how best to advance the homeland security enterprise to meet today's environment. Plenaries, breakout sessions, and lightning rounds featured thoughtful discussions on specific aspects—from the changes to the threat environment, both where threats emanate from and what is targeted, to promoting process improvements and resilience.

This report is intended to provide an overview of the ideas and recommendations raised during the HSEF. To make this more accessible, this report consolidates the session results into four topical themes. The table below provides mapping for how each session contributed to each of these topical themes.

Topical Theme	Contributing Sessions
Mitigating Geopolitical and Economic Risk	Plenary: Addressing Foreign Investment Into & Out of the United States* Plenary: Supply Chain and Critical Infrastructure Resilience Investments* Breakout: Financial Services Track Breakout: Supply Chain Risk Management and Critical Infrastructure Resilience*
Enhancing Transportation, Travel, and Trade	Plenary: Border Security and CBP's Competing Missions Plenary: Emphasizing Partnerships in DHS Customer Experience* Plenary: Collaboration Against Emerging Threats* Breakout: Aviation Security and Cybersecurity Track Breakout: AI & Customs Breakout: Future of Travel
Increasing the Cybersecurity Baseline by Reducing Burden	Plenary: AI-Enabled Cybersecurity Plenary: AI: Setting the Stage for Rapid Development and Adoption Plenary: Supply Chain and Critical Infrastructure Resilience Investments* Plenary: Collaboration Against Emerging Threats* Breakout: Supply Chain Risk Management and Critical Infrastructure Resilience* Lightning Round: Digital Identity Security and Innovations
Advancing the Enterprise Through Multidisciplinary Expertise	Plenary: Collaboration Against Emerging Threats* Plenary: Emphasizing Partnerships in DHS Customer Experience* Plenary: Advancing the Homeland Security Enterprise Lightning Round: Center for Prevention Programs and Partnerships (CP3) Lightning Round: The Terrorism Liaison Officer Program

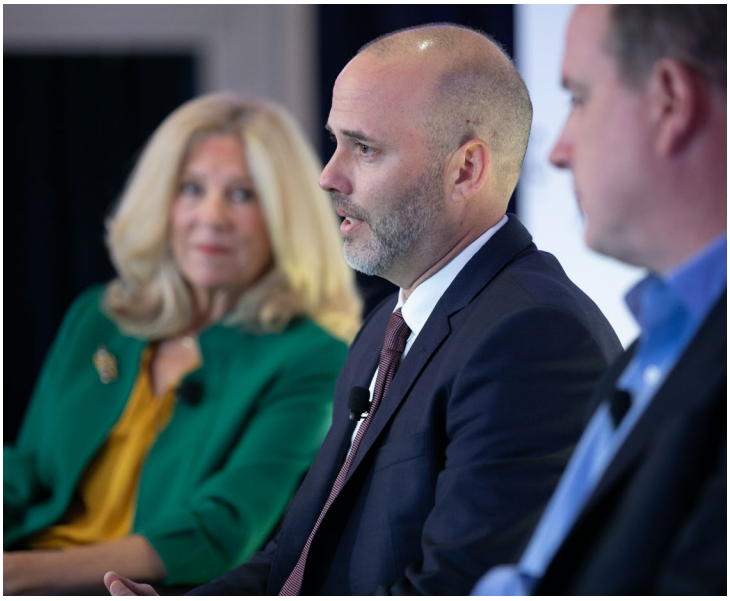
*Indicates the session contributed to more than one theme.

MITIGATING GEOPOLITICAL AND ECONOMIC RISK

Across the two days of the conference, HSEF panelists and participants repeatedly turned to the changes they are seeing in the threat environment and how that influences their focus on what should be done to mitigate it, and how. Geopolitical and economic risks topped the list.

To describe the geopolitical aspect of this change, participants contrasted today's environment with our historical views as a nation. Since World War II, US international policy was based on the premise that economic interdependence leads to market efficiencies as well as global stability, with the assumption that countries would value their economic growth development over aggression. Historically, congressional leaders of both parties have encouraged—and provided benefits to—US companies to outsource components of their businesses to emerging nations in order to foster these ties, setting the stage for a sustained period of international stability. US companies took advantage of these opportunities to outsource factories, development, and low-wage jobs. In places like China, the government in turn committed land, low-cost supplies, and personnel. Capital markets also followed suit with US companies and investors moving funds outside of the US to maximize their return.

Recently, however, the Chinese government has become more overt in advancing its view of how the future world order should operate. It has increasingly pressured companies to turn over their technologies and intellectual property, reduced non-Chinese employees, and even threatened to seize the factories of US-owned companies. In contrast, the US does not have the legal framework to mirror sanctions in response to efforts and sanctions placed on US-owned businesses in other countries. One of the only successful ways that the US has been able to respond to the threat posed by China has been to use "Rip and Replace" legislation, which provides funding to US companies to "rip out" telecommunications equipment from Chinese companies and "replace" it with equipment from US and allied nation manufacturers.



HSEF participants also emphasized that natural disasters pose significant economic risk. As an illustration, the COVID-19 pandemic demonstrated the challenges to the US supply chain. In particular, the pandemic highlighted the risk of overreliance on a single manufacturer or country. During the pandemic, China and other countries the US has long relied on for manufacturing critical infrastructure items (i.e., medical supplies) shuttered their factories, closed their borders, and limited international trade and transportation. The pandemic also highlighted how limited a view many US companies have into their supply chains. While they may know their immediate suppliers, they often do not know their suppliers' suppliers. While the pandemic showed companies and the federal government the need to invest in resilience, develop continuity of operations plans, and mitigate the risk of their operating ecosystem, the degree to which they have done so is uneven, leaving significant vulnerabilities.

Over the past decade, China and other nations with adverse interests have asserted their renewed willingness to use military solutions, as well as economic ones, to advance their interests. As tensions between these two nations continue to rise, the US must consider the level of risk present, how we can best reduce our vulnerability or mitigate potential consequences should the US and China move toward direct hostilities, and how US-owned companies can better position for the current threat environment.

Actions/Recommendations:

- Congress should consider statutorily authorizing an agency to produce a geostrategic risk rating for US-owned companies, based on their supply chain and financial dependence on countries who advance their interests through adverse means. Companies with higher risk ratings could be subject to higher levels of federal oversight, required to have increased capital to offset their risk, and/or required to carry additional insurance.

- Congress should consider additional tax and economic incentives to companies that make significant investments to reduce their reliance on production in countries with adverse interests. Qualifying investments might include skills development for US personnel, additional US hiring, and investments in technology/automation to reduce dependency on cheap labor overseas.

- Congress should authorize, or the Administration should direct, an agency to conduct an education campaign for US consumers on the risks of dependency on products produced by international adversaries, similar to the campaigns aimed at educating consumers about child labor.

- Congress and federal agencies must work with private businesses and relevant stakeholders to provide legislative and regulatory flexibility during disaster response, providing companies the ability to restore critical supply chains faster. As part of this exercise, they would develop parameters for when that flexibility would be exercised and expectations for returning to a steady state.

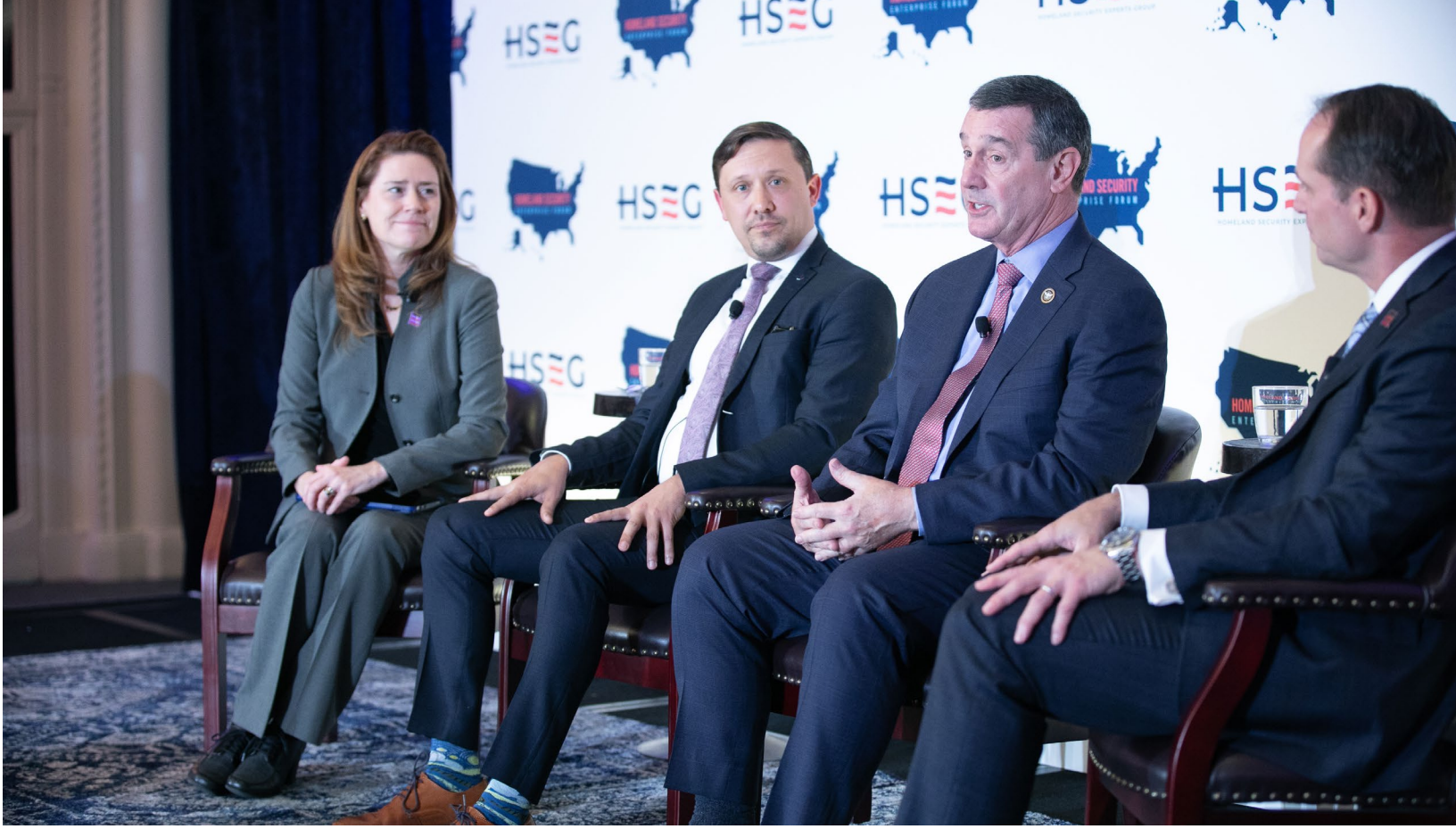
- The Administration should complete its update of PPD-21 "Critical Infrastructure Security and Resilience"[1]—broadening it to include supply chain challenges, today's state and nonstate actors, and enhancing its all-hazards approach.

- Supply chain resilience as a mission must be better defined and appropriately accounted for within DHS. While cybersecurity and infrastructure security are specifically identified within the Cybersecurity and Infrastructure Security Agency (CISA) mission, supply chain resilience is not.

- Federal agencies should consider how to better incentivize investment in supply chain resilience, such as considering resilience as a factor in awarding grants and contracts. The Federal Emergency Management Agency (FEMA) and CISA should provide guidance to state and local governments encouraging adoption of similar policy.

- US companies should undertake the effort to document the entirety of their supply chains, including identifying not only their provider companies, but the providers they use, along with their locations. Companies should use this information to develop an all-hazards multi-layer contingency plan(s) that are exercised to ensure resilience in the face of an unplanned natural disaster or deliberate attack.

[1] Presidential Policy Directive 21- Critical Infrastructure Security and Resilience | whitehouse.gov (archives.gov). https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.



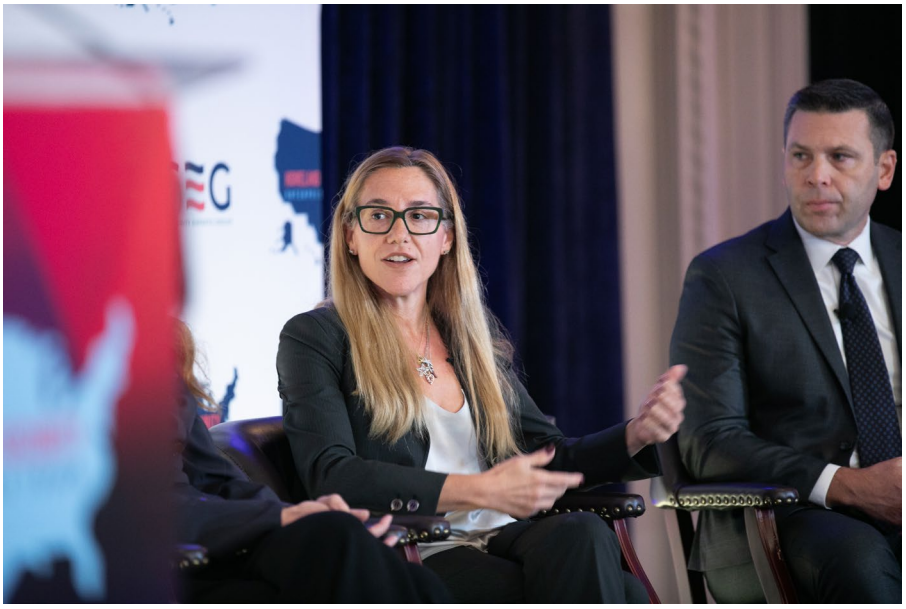
ENHANCING TRANSPORTATION, TRAVEL, AND TRADE

Over several sessions, HSEF participants discussed the importance of transportation, travel, and trade to our economy, and focused on opportunities to advance customer experience, create a more agile security environment, and change or streamline processes to meet expected increases in capacity needed over the next decade. The sessions explored how the forward-leaning and ethical use of data and automation, as well as reinvestment of human capital in higher-risk areas can meet the security, volume, and customer experience needs anticipated for Transportation Security Administration (TSA) and US Customs and Border Protection (CBP).

Government agencies and industry associations predict that air travel will fully recover its pre-pandemic level in 2024, and will continue to increase. Air cargo volume also increased during the pandemic and continues to remain high. These increases will impact the entire continuum of travel of people and cargo from initiation of transit through final destination. Participants emphasized that these projections, coupled with adversaries' changes in tactics to advance their continued desires to attack the homeland, have created the opportunity for government, the private sector, and industry to build new processes and ways of doing business.

Participants emphasized how artificial intelligence, machine learning, and other automation could decrease the burden on personnel from rote, time-consuming activity—in which humans are more likely to make mistakes. This would free personnel to focus on situations that require investigation and judgment. For example, TSA is leveraging "open architecture" (i.e., vendor agnostic standards for data) and artificial intelligence or machine learning algorithms to identify suspicious

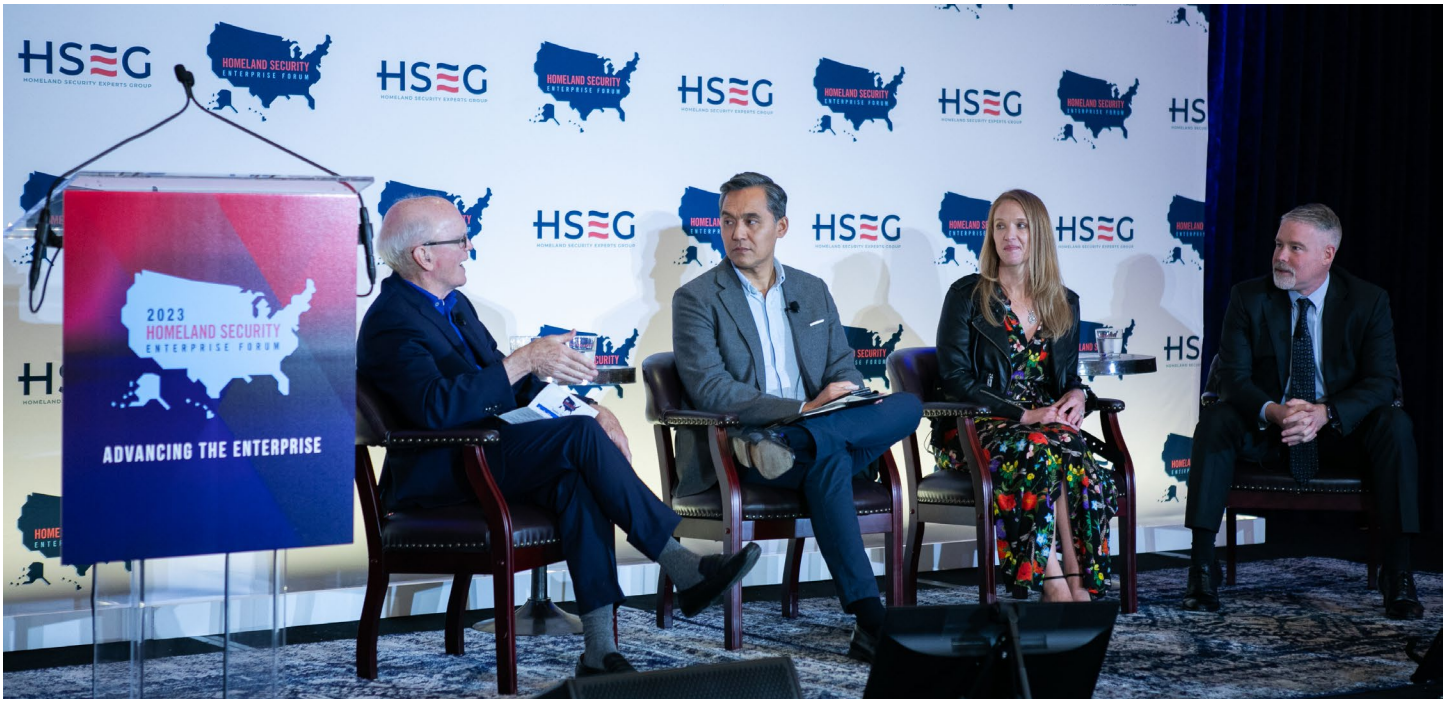
items and anomalies. CBP has also identified opportunities to leverage artificial intelligence or machine learning to expedite screening of cargo on ships, planes, trains, and trucks entering the country, allowing officers to focus on resolving issues identified.



Participants also focused on opportunities to enhance the customer experience. They emphasized the continued focus on pre-screening—such as TSA's PreCheck® and CBP's Global Entry—as a way to identify those who are less of a threat, and provide them a differentiated experience. Of note was TSA's One-Stop initiative, which will allow passengers who were screened overseas at an airport whose security is found commensurate with the US, to proceed directly to any domestic flight without having to be rescreened. This not only frees up TSA resources to focus on higher priority threats, but it will also increase airport capacity and productivity within existing real estate limitations. Similar opportunities exist to enhance the traveler's journey beyond interaction with the government, incorporating changes in processes and traveler flow as US airports expand or renovate.

Actions/Recommendations:

- DHS should continue efforts to determine how to best implement the Homeland Security Advisory Committee recommendation to "Consolidate and Optimize Trusted Traveler Programs" (See Customer Experience and Service Delivery Final Report (dhs.gov)).
- TSA should continue its effort to increase the percentage of travelers enrolled in TSA PreCheck, and appropriately align resources at checkpoints to ensure TSA PreCheck members receive the expected speed and experience.
- As DHS looks to further incorporate artificial intelligence or machine learning, it should proactively expand its efforts to explain what data is collected, how it is being used, what the benefits to travelers are, and what protections exist for their information. DHS should continue to emphasize when travelers have the option to opt out of automated processes, such as biometric collection.
- DHS should proactively explain how it will test artificial intelligence and machine learning, ensuring ethical and privacy concerns are taken into account, and how it will report results publicly in a format understandable to and accessible by the public that DHS serves.



INCREASING THE CYBERSECURITY BASELINE BY REDUCING BURDEN

Panelists highlighted a series of lessons learned—both in terms of our view of the threat, as well as what needs to be done to prepare, mitigate, and respond—from recent cyberattacks, such as the Colonial Pipeline ransomware event.

HSEF participants emphasized that the ability of small and midsize businesses to increase their cybersecurity posture was critical to critical infrastructure protection. Small and midsize businesses own approximately 90% of the critical infrastructure in the US, but many do not invest sufficiently in their cybersecurity, due to a lack of resources and infrastructure. One of the primary resource shortages is staff with the requisite expertise. IT and cybersecurity personnel are responsible for sifting through large amounts of data, conducting rapid assessments, and prioritizing security threats. This leads to burnout, rapid staff turnover, and insufficient efforts to promote knowledge management and transfer. Given their size, small and midsize companies often face the tradeoff of taking limited resources offline for training, knowing training is needed to keep up with changing threats. Participants also mentioned that small and midsize businesses suffer from "patch fatigue" and other vulnerabilities that leave their systems more accessible to cyberattacks. Many small and midsize businesses rely on out-of-the-box solutions and assume they are safe, instead of regularly updating software and applications and verifying program codes. They also tend to limit cyberthreat training to phishing, spam, and typical hacking strategies.

Nefarious actors take advantage of cyber fatigue and simplistic training. Participants noted that approximately 90% of cyberattacks, including some of the most detrimental recent ones, have started with a human connection. Actors leverage AI to create tailored communications and send targeted messages that sound like they are coming from a human, making it that much harder to detect. These actors then get environmental access to critical data.

Exacerbating the problem is that companies are often hesitant to admit they have been breached. This prevents them from working with one another and/or the federal government to determine where the threat started, how to limit the damage, and how to patch the issues along the way.

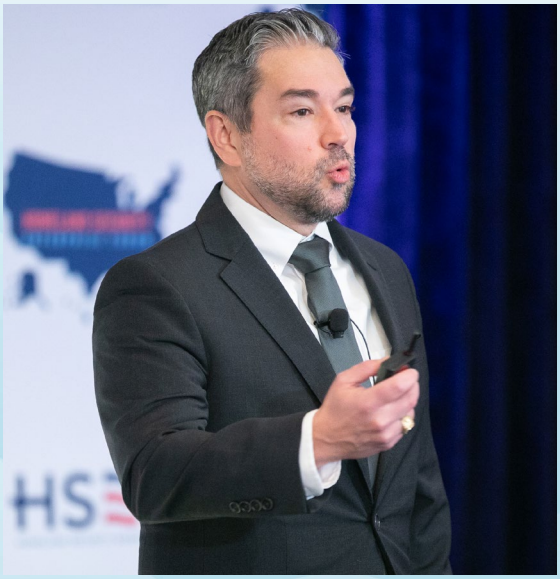
The efforts to protect transportation infrastructure after the Colonial Pipeline cyberattack, in contrast, highlights how partnership between the federal government and industry can change these dynamics. Industry partners noted that their ability to quickly contact and engage with federal stakeholders is critical to protection, mitigation, and response. TSA's unique regulatory framework was highlighted as one that better supported engagement as well as rapid response in emergency situations. Panelists noted that relationships developed through collaboration on prior threat streams have provided a model to follow for cyber, where industry partners and TSA can work through both threats and solutions, modifying the approach to achieve better outcomes and increased ability for compliance.

Cybersecurity requires open and transparent communication between industry partners and the federal government. Without better mentoring of existing cyber talent, and investment in capabilities and infrastructure (particularly for small and midsize businesses), the critical infrastructure of the US will remain vulnerable to cyberattack.

Actions/Recommendations:

- Relevant federal government agencies should, in cooperation with large businesses, use cybersecurity partnerships to share best practices and lessons learned in how to implement cybersecurity protections with small and midsize businesses to enable them to more rapidly enhance their security posture.
- Small and midsize businesses should explore leveraging artificial intelligence or machine learning to help secure their infrastructure, freeing up personnel to tackle more complex cyber issues. The federal government should develop a commonly accepted set of standards, or regulatory framework, for use of artificial intelligence or machine learning, particularly regarding mitigating cyber risk.

ADVANCING THE ENTERPRISE THROUGH MULTIDISCIPLINARY EXPERTISE



Leveraging partners beyond traditional law enforcement, and including industry in long-term federal planning, were identified by HSEF participants as essential to advancing the homeland security enterprise. HSEF sessions explored the integration of approaches from a variety of disciplines to think differently about the threat and protect communities across every level of society.

Given the evolution of the threat both domestically and internationally, the homeland security enterprise must think creatively and expansively about the partners with whom to engage. For example, the DHS Center for Prevention Programs and Partnerships (CP3) has embraced this concept, employing a multidisciplinary and public health-informed approach to prevent targeted violence and terrorism.

Recognizing that the discipline of prevention requires the involvement of society-wide partners, rather than relying solely on law enforcement and criminal justice to keep communities safe, CP3 has broadened its partnerships to include mental health providers, teachers, religious leaders, etc. By embracing this multidisciplinary approach, CP3 can provide tailored assistance based on individuals' behaviors, not ideologies expressed, to prevent targeted violence and terrorism.

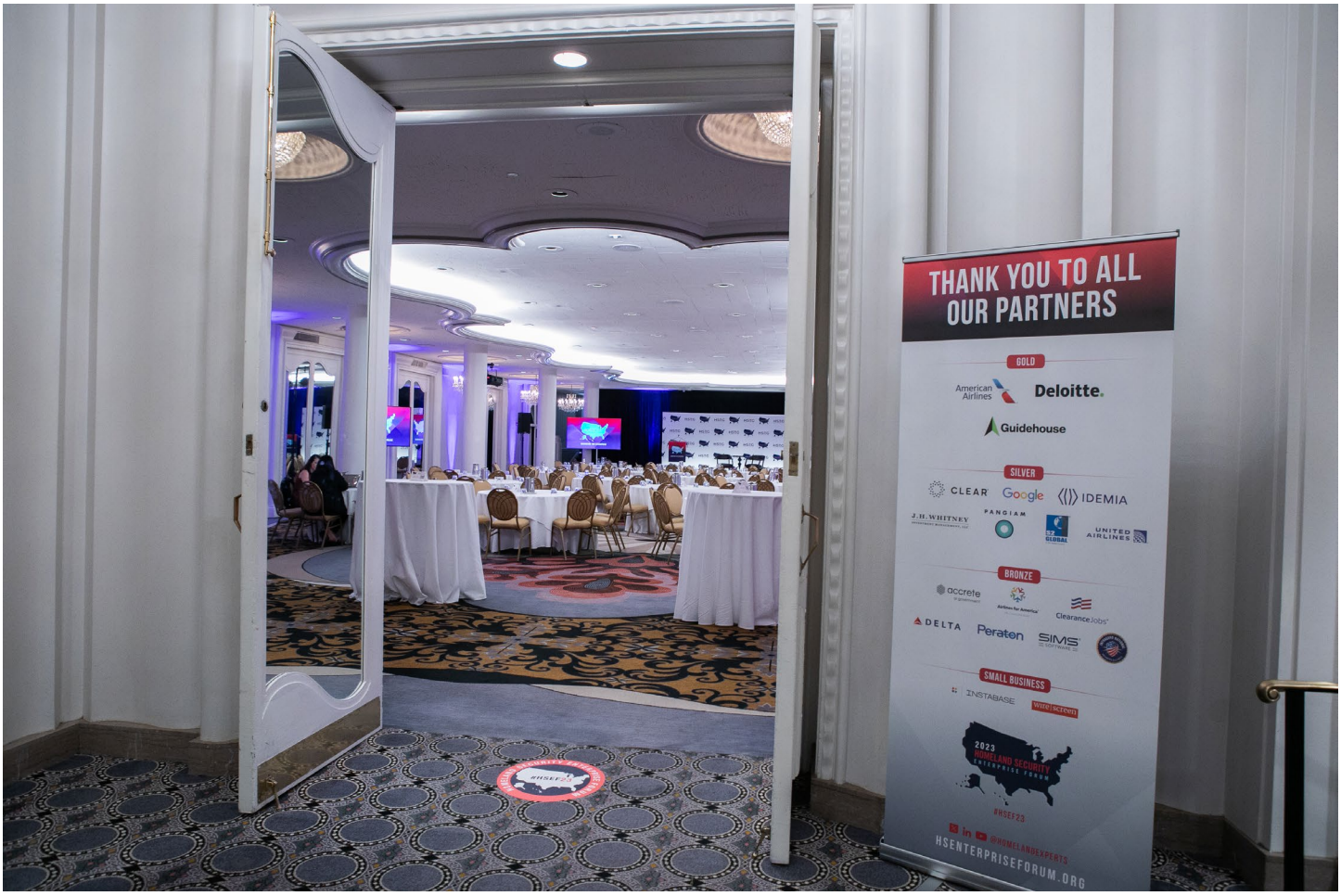
Similarly, DHS fusion centers have focused on training not only public safety personnel but also relevant stakeholders, including small and midsized businesses and critical infrastructure personnel, on spotting the indicators of terrorism, how to complete suspicious activity reports, the intelligence cycle within fusion centers, and privacy and civil liberties considerations. Often, these partners do not know how they fit into the larger picture of prevention and where and how they should report suspicious activities. Through this program, fusion center personnel help bridge that knowledge gap and build necessary partnerships to keep the homeland safe.

Through the release of its Capital Investment Plan and Roadmaps, TSA creatively signals to industry how they intend to make investments to reach full operational capacity and mitigate future anticipated risk. Industry partners, such as airlines or airports, can then also make investment plans accordingly, ultimately maximizing their returns by ensuring future plans are aligned with intended regulation and security best practices.

The space between industry, not-for-profit organizations, private sector, and government continues to shrink as the threat evolves. The more these entities work together collaboratively across all levels of society, the better prepared the US will be for disasters, whether manmade or naturally occurring.

Actions/Recommendations:

- Stakeholders across the homeland security enterprise should continue to identify opportunities to engage nontraditional stakeholders, broadening the expertise available to tackle today's threats.



CONCLUSION

Geopolitical tensions with nation states, recent disasters, and cyberattacks against US-owned businesses demonstrate that threats to our homeland continue to increase in complexity, involving a larger number of targets affected, actors implicated, and vectors at risk. The attacks in Israel serve as a stark reminder of the dangers still posed by committed terrorists and the continued need for vigilance and ongoing assessments of the risks we face as a nation.

The homeland security enterprise must continue to evolve its approach to counter the current and emerging threats through the open exchange of ideas, recommendations, and proposed action between industry and government, and traditional and nontraditional stakeholders. No one entity can do this alone.

The Homeland Security Experts Group will continue to facilitate the public-private partnerships, drive conversation, and lead engagements to advance the recommendations and actions included in this report. Homeland security is evolving, and the Homeland Security Experts Group, HSEF attendees, and all stakeholders play a critical role in contributing to ensuring the safety, security, and resilience of our nation. By focusing on enhancing and expanding partnerships and thinking differently about the threats, we can best keep the homeland safe while respecting our fundamental national traditions and rights.