SESSION RECOMMENDATIONS

SECURITY THROUGH PARTNERSHIP

PRESENTED BY

Guidehouse
Outwit *Complexity*

THANK YOU

This report was prepared by The Homeland Security Enterprise Forum with the support of Guidehouse. We would like to acknowledge:

Guidehouse Report Authors:
Patricia Cogswell | Briana Petyo Frisone | Donna Roy
Ben Gorban | Caroline Bracken

Guidehouse Report Editors:
Cara Cancelmo | Fouad Pervez

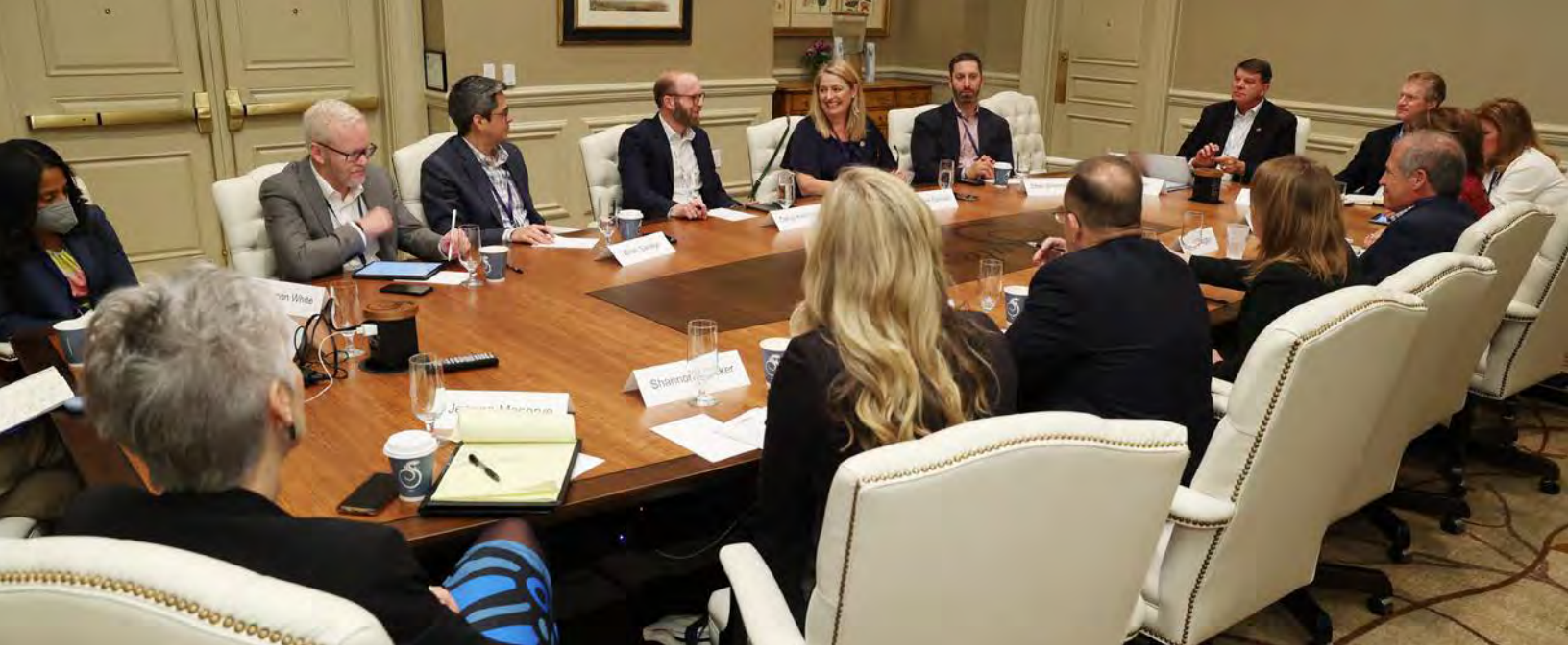
Guidehouse Notetakers:
Caroline Bracken | Cara Cancelmo | Ben Gorban | Daniel Ingley
Linzy Kraemer | Wendy Robinson

The forum takes great pride in engaging the nation's rising leaders in the homeland security space. The American University volunteers played a crucial role in notetaking and production of the forum, and was led by Dr. Trace Lasley, Professor of Practice in the Department of Justice, Law, and Criminology in American University's School of Public Affairs.

American University Volunteers:
Eliot Bradshaw | Anna Christy | Tatiana Eastin | Connor Lemcke
Andrew McCoy | Julia Mullert

SECURITY THROUGH PARTNERSHIP

TABLE OF CONTENTS



EXECUTIVE SUMMARY

The 2022 Homeland Security Enterprise Forum (HSEF) was held exactly one month before the 20th anniversary of the signing of the Homeland Security Act of 2002, which officially created the Department of Homeland Security (DHS). When DHS was created, it established five guiding principles that shape the mission of the Department:

1. Champion 'Relentless Resilience' for All Threats and Hazards;
2. Reduce the Nation's Risk to Homeland Security Dangers;
3. Promote Citizen Engagement and Strengthen and Expand Trusted Partnerships;
4. Uphold Privacy, Transparency, Civil Rights, and Civil Liberties; and
5. Ensure Mission-Driven Management and Integration.[1]

The second annual HSEF aligned with these guiding principles. The overarching theme of the Forum was *Security Through Partnership*. Over the three-day Forum, subject matter experts from government, public, and private sectors provided strategic thought leadership on the value of partnerships in the homeland security enterprise today and how to build and enhance partnerships to face evolving threats. Almost unanimously, when asked to identify a solution to addressing a threat, enhancing resilience, upholding privacy and civil rights and liberties, enhancing technology, and identifying promising practices, participants acknowledged the value and importance of partnerships. The Forum focused on the successes of relationships, methods to enhance current partnerships, relevant stakeholders with whom to foster new partnerships, and ways partnerships within the federal government and between federal agencies and relevant stakeholders could continue to secure and protect the homeland.

Identifying and mitigating emergent manmade and natural disasters and threats, maturing the homeland enterprise to reduce the nation's risks, and recognizing the future of the mission space were also strong themes throughout the forum. In many cases, the discussions also identified opportunities and recommendations to more proactively counter threats and enhance resilience should an incident occur. Plenaries and breakout sessions that centered on new and emerging technologies and data also included conversations about the importance of protecting civil rights and civil liberties, ensuring that government and business stakeholders were transparent with the community about what information was being collected, how it was being used, and how their privacy was being protected.

[1] https://www.dhs.gov/guiding-principles

This report highlights the conversations that took place across the plenaries and breakout sessions throughout the HSEF and captures the key takeaways and recommendations that resulted from discussions. These takeaways and recommendations should establish priorities and guide the homeland security enterprise over the next 12 months.

For reading ease, rather than reporting by individual session, this report consolidates the primary points of agreement, key "takeaways," and recommendations by topic. The table below provides a short mapping of how materials from each session contributed to the report sections below:

PRIMARY	TOPIC	CONTRIBUTING SESSIONS
Identifying and Mitigating Emergent Threats	Domestic Violent Extremism	Plenary: Understanding the DVE Threat Landscape Breakout: Understanding and Mitigating the Domestic Violent Extremism Threat to the National Security Enterprise
Identifying and Mitigating Emergent Threats	Countering Transnational Organized Crime and Securing the Western Hemisphere	Plenary: Securing the Western Hemisphere through Policy and Technology Plenary: Homeland Defense and Security – Reframing Our Concepts Plenary: Partnerships in Counter-Human Trafficking Efforts Breakout: Leveraging Data and Information Sharing to Counter Transnational Organized Crime Breakout: Countering Human Trafficking
Identifying and Mitigating Emergent Threats	Cyber and Artificial Intelligence	Plenary: What's in a Name: Critical Infrastructure Protection…or Resilience? Plenary: Quantum Computing: Homeland and National Security Ramifications Breakout: Transitioning Technology to Enable the Homeland Security Enterprise Breakout: Cyber Supply Chain Security Breakout: The New Arms Race: Post-Quantum Cryptography
Identifying and Mitigating Emergent Threats	Countering Unmanned Aerial Systems	Breakout: Addressing the Growing Threat of sUAS Breakout: The Future of Travel Roundtable
Maturing the Homeland Enterprise		Plenary: Information Sharing: Adapting the CT Enterprise for Today's Threats Plenary: FBI: Maximizing Collaboration Against Our Modern Threats Breakout: Bridging DHS Mission Areas Through Data Breakout: Toward a Strategy for National Security Emergencies Breakout: Renewing FISA
Future of the Mission Space	Trade	Breakout: The Future of Trade
Future of the Mission Space	Travel	Plenary: The Future of International Travel Breakout: The Future of Travel Roundtable
Future of the Mission Space	Disaster Resilience	Breakout: Current and Emerging Issues in Disaster Resilience

IDENTIFYING AND MITIGATING EMERGENT THREATS

The United States faces continuous risks from known and evolving threats. The individuals and groups seeking to perpetrate these attacks can create catastrophic problems negatively impacting entire organizational sectors and regions, and can launch these attacks locally, or from across the globe. Participants broadly agreed the threats are physical and cyber; domestic and abroad; perpetrated by state and non-state actors, transnational organized criminals, extremist groups, and lone wolves. Discussions identifying and mitigating emergent threats centered on domestic violent extremism (DVE); transnational organized crime, including human trafficking organizations; countering unmanned aerial systems (CUAS); and the benefits and concerns of cyber, artificial intelligence (AI), and quantum computing.

DOMESTIC VIOLENT EXTREMISM

DVE perpetrated by groups and individuals inspired by the entire spectrum of political and ideological beliefs has increased measurably. DVE groups have carried out attacks against federal and local law enforcement officers and buildings, the US Capitol, elected officials, local election officials and their families, schools and workplaces, and faith- and community-based centers.

Participants discussed the critical role social media plays in enabling the frustration of individuals to reach a wider audience, which creates a self-perpetuating system that escalates tensions. Foreign actors have also exploited this environment to influence and erode faith in the US government and democracy. To deter the escalation of tensions and divisiveness, participants advocated that officials take action to call out dis-information, particularly when politicians clearly use it to incite or support violent and criminal behavior. Participants also highlighted the need to explain the risk posed by foreign influence transparently and suggested identifying and adopting a common purpose and positive feedback loop to counter this trend, ultimately leading to a reemergence as a more unified nation.

Another topic of discussion included the importance of continuing efforts to enhance the community's understanding of the threat landscape and the variety of actors involved through rigorous information collection and analysis, and widespread sharing. Participants discussed increased resources in fusion centers to collect and synthesize data identifying potential risks of violence, and to similarly increase the resources and personnel in the federal government to share relevant information about the DVE threat. Most participants highlighted that effective information sharing requires developing and maintaining relationships with counterparts in other agencies, including knowing when to pick up the phone to intervene prior to an event in addition to analyzing data and being aware of trends identified in reporting. This applies to not only government officials, but also in business and civil society, especially for DVE. All participants emphasized the critical nature of building new, and maintaining existing, partnerships.

Participants also identified the need to continue leveraging partnerships to expedite research, identify promising practices, and strategically share the resources needed to continue protecting the nation. Participants also acknowledged some employees of US security institutions have participated in recent DVE incidents or have supported violent extremist ideologies. These participants discussed the importance of being transparent with the community and taking actions to address the insider DVE threat. As a point of additional concern, participants noted that while there is significant data regarding the scale of the threat of DVE in US security institutions, the security community has wrestled with how to use it, given the potential implications.

DVE RECOMMENDATIONS:

- **DHS and DOJ should invest in research quantifying the likelihood that online rhetoric will lead to offline violence, and then use those indicators to determine actions to intervene.**
- **All must routinely call out and condemn incitement of violence and criminal behavior. Federal law enforcement agencies should appropriately investigate actions of politicians who incite or support violent and criminal behavior.**

COUNTERING TRANSNATIONAL ORGANIZED CRIME AND SECURING THE WESTERN HEMISPHERE

Transnational organized crime and human trafficking are multi-billion-dollar enterprises affecting communities and nations worldwide. Participants discussed the increasing complexity and sophistication of transnational organized crime groups, which apply their knowledge and experience from trafficking drugs and firearms to the trafficking of people. Transnational organized crime groups continue to evolve and adapt, using the latest technologies to expand their profit-making illicit endeavors. Their ever-changing methodologies create challenges for those charged with countering their illicit activity.

Participants discussed how the changing drivers of the migration surge at the southwest boarder, including increased economic and political instability caused by COVID-19, challenge US infrastructure, legislation, and processes. Demographics also continue to change. Countries in Central and South America have surpassed Mexico as the country of origin, and Venezuelans who previously migrated to Central America have now undertaken a second migration to the US. Participants agreed a holistic review of data over time would show how flows and smuggler tactics change and would improve the government's ability to respond. Participants largely agreed that the government constructed policies and processes based on a primarily Mexican-based migration flow, which allowed for CBP agents to rapidly repatriate individuals. The change in demographics has created significant backlogs as US officials work to evaluate a record number of arrivals and claims of asylum and return the increased numbers of people, who aren't eligible for entry under current law, to their countries of origin.

Separately, participants discussed how environmental complexities impede governments' and non-governmental organizations' abilities to collect data that would enable a holistic understanding of the scope and scale of human trafficking, as well as the mechanisms traffickers use to perpetrate their crimes and shelter their proceeds. Participants also discussed how criminal statutes further victimize those being trafficked, rather than focusing on the perpetrators. This allows traffickers to revictimize and retain

their hold on vulnerable individuals. Panelists and breakout session participants emphasized the need to systematically and regularly review the factors making people vulnerable to human trafficking and update measures to counter them.

Participants concurred educational efforts about human smuggling/trafficking need to be improved. Participants credited federal law enforcement and US Attorney's Offices with making concerted efforts to educate state legislatures and local attorneys on federal prosecution thresholds and guidelines. Participants also recognized the work the federal government has done to provide state, local government, and private organizations with information identifying trafficking, how to report it, and how to intervene. However, participants stressed the need to reach potential trafficking victims through educational and public service campaigns and to provide services to survivors. It was noted when the Nationwide Suspicious Activity Reporting program started, law enforcement agencies were educated about the importance of completing reports and sharing information, but that has since decreased, which has impacted the ability to develop holistic pictures of the criminal threats.

Participants suggested the development of awareness campaigns reminding business stakeholders that, although cheap labor may improve profits, it could encourage labor trafficking. Participants also noted that many individuals may not know they are at risk of being trafficked, that they are being trafficked, or that services exist to help them. Participants suggested the use of data analysis to identify geographic areas where trafficking will more likely take place to target educational and awareness resources. Victim services organizations and law enforcement stakeholders could enhance their collaboration to provide victim-centric programs for those who have been trafficked and additional access to trauma systems, treatment, and social services. These programs should highlight law enforcement protections available to victims, such as special immigration status, which encourage human trafficking victims to work with law enforcement to identify and prosecute perpetrators.

COUNTERING TRANSNATIONAL ORGANIZED CRIME AND SECURING THE WESTERN HEMISPHERE RECOMMENDATIONS:

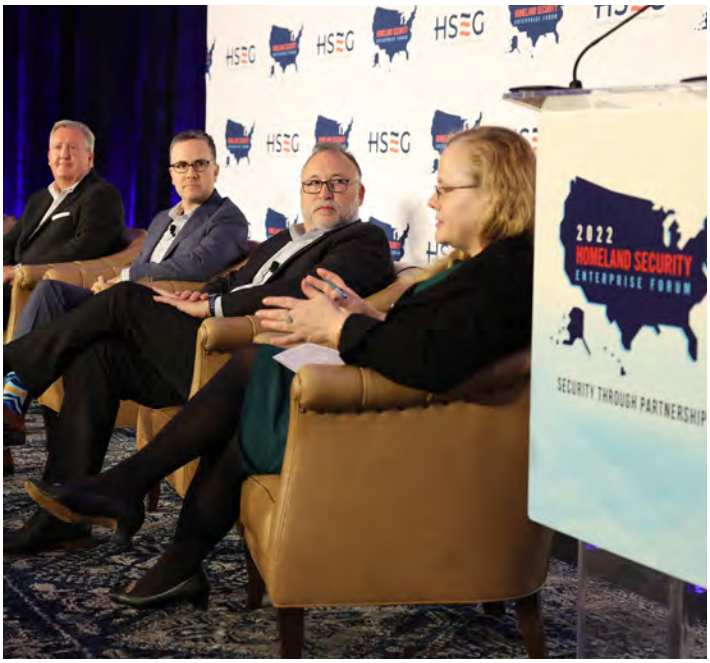
- **Invest in legal, policy, organizational, and facility changes to adapt to the evolving Western Hemisphere migration demographics and threat environment.**
- **Codify the Human Trafficking Act, which will provide more resources and funding to counter human trafficking.**
- **Update policies and criminal statutes to recognize human trafficking victims as such, instead of criminals. Currently, 14 states allow for the arrest of underage trafficking victims and some statutes do not differentiate sex trafficking from prostitution.**
- **Develop strategies and effective policies to better enable the use of open-source data critical to dismantling Transnational Criminal Organizations (TCOs). TCOs leverage social media and dark web platforms to advance their criminal enterprises, which enables new tactics and techniques faster than the policy framework and allowing law enforcement and intelligence entities to use the data.**

CYBER AND ARTIFICIAL INTELLIGENCE

New and emerging technologies have profoundly impacted business operations, trade, migration, economies, and partnerships. Business and political leaders at all levels have leveraged this increasing interconnectedness to innovate faster and more creatively, to address emerging vulnerabilities, and to build national and international security partnerships.

Participants overwhelmingly focused on cyber, AI, and quantum in discussions about these new and emerging technologies. It was noted that three areas of quantum exist: 1) computing, 2) communications, and 3) sensing, which all live at different stages of maturity. Participants noted the importance for all stakeholders to acknowledge the possibilities of quantum. Quantum computing has the ability to identify potential solutions to large-scale issues, including genetic research and drug and vaccine design, in a matter of minutes. These opportunities present significant benefits to both the US government, businesses, medical and educational stakeholders, and society as a whole, as was demonstrated when countries and companies integrated multiple ongoing workstreams to respond to the COVID-19 pandemic.

Participants also noted that cyber, AI, and quantum present significant risks. In 2021, the global estimated cost of cyber attacks, of which the US public sector represented a significant portion, was $6 trillion. Too often, security is an afterthought, not a forethought. Additionally, challenges associated with insufficient encryption, poorly understood algorithms, and failure to adequately address ethical and cultural changes at speed, continue to impact US efforts advancing policy and capability. Participants stressed risk-based management in segmenting vendors to best support and protect critical business activities and the need for organizations to stay agile in their approach to supplier risk management. They centered on the notion that protection requires a variety of solutions, including segmentation, micro-perimeters, and other means of controlling access to



information in different places, as opposed to just firewalls. Policy enforcement using tools and processes remain vital for providing a seamless user experience and helping address the lack of people, funds, and inefficiencies.

Conversations also focused on the need for transparency and accountability when attackers breach systems. Business participants acknowledged that many organizations tasked with protecting critical infrastructure don't have cyber experience, fully understand the complexities, or know what and whom to ask. The conversations also noted that government and businesses must prioritize protecting the most critical infrastructure and the elements that can't afford to be lost before addressing what remains with residual resources. Not everything can be protected, but it is time to address and plan for it for an attack with available resources.

Many participants supported the need for the federal government to create a data science career path to entice interested individuals and invest in the hiring and training of analysts and law enforcement to increase the effectiveness in countering threats using more sophisticated analysis of data. Specifically, participants agreed the government should hire people with varying backgrounds, not just a physicist or a cyber expert, who can understand quantum and apply it, as well as individuals who understand how

to utilize the capability and make sure it's maintained and upgraded regularly. Participants encouraged a continued focus on these areas, as well as rapidly developing on-the-job training and dedicated career paths. Participants emphasized that these investments could not wait, recognizing that we have a limited window before our adversaries capitalize on our weaknesses.

Participants noted business stakeholders and government organizations must broadly encourage and provide trainings. Coordination between business and government to identify bad actors and engage in mitigation strategies before an attack is critical. Relationships are essential at the local, regional, and national levels to enable this level of coordination and collaboration. Education, training, and awareness have all increased significantly, as have our responses.

In addition to personnel and training development, participants pointed to the need for federal statutes and regulations ensuring organization implement new technologies securely and appropriately. This included the desire to establish a mechanism to continuously upgrade quantum standards, with the goal of reaching "quantum-safe algorithms" now, while the possible risks in terms of national security remain manageable. Participants also confirmed clearly defined roles and responsibilities related to crypto and quantum in the US government do not exist. Participants identified multiple national strategies, state and local strategies and plans, and private companies with their own plans, but coordination remains limited. To address this issue, the Department of Defense or NIST could lead governing components. Especially with the challenges of increased information sharing, recruitment, and limited employees, there needs to be a clear leader when breaches occur.

CYBER AND ARTIFICIAL INTELLIGENCE RECOMMENDATIONS:

- **Prioritize awareness and policies addressing the intersection of quantum and national security policy in the counterintelligence space.**
- **Establish a whole of government process to review quantum and AI and make recommendations for governance. It is important to find the right balance between incentives and mandates in cyberspace, along with balancing responsibility for resiliency between the private sector and the government.**
- **Promote investment in recognized areas that provide benefits, such as creating third-party mechanisms to verify and validate breach reports and establishing standard software bill of materials (SBOM).**
- **Identify opportunities to continue creating pathways for innovation by increasing collaboration between Government and non-governmental partners, including federally-funded research and development centers (FFRDCs), in target opportunity areas, optimizing the initiatives by the likelihood of transitioning projects into implementation.**
- **Invest in public-private partnerships working across DHS operating components to continue driving innovation and efficient operations, such as open architecture innovation for training data for machine learning that cross multiple use cases (including the future of travel, infrastructure, combating transnational crime, and reducing human trafficking as relevant threats).**
- **Join forces with interested federal agencies, such as the Department of Energy, to combine investments and strategies that address the near term and stay ahead of threats by collaborating on long-term initiatives.**

COUNTERING UNMANNED AERIAL SYSTEMS

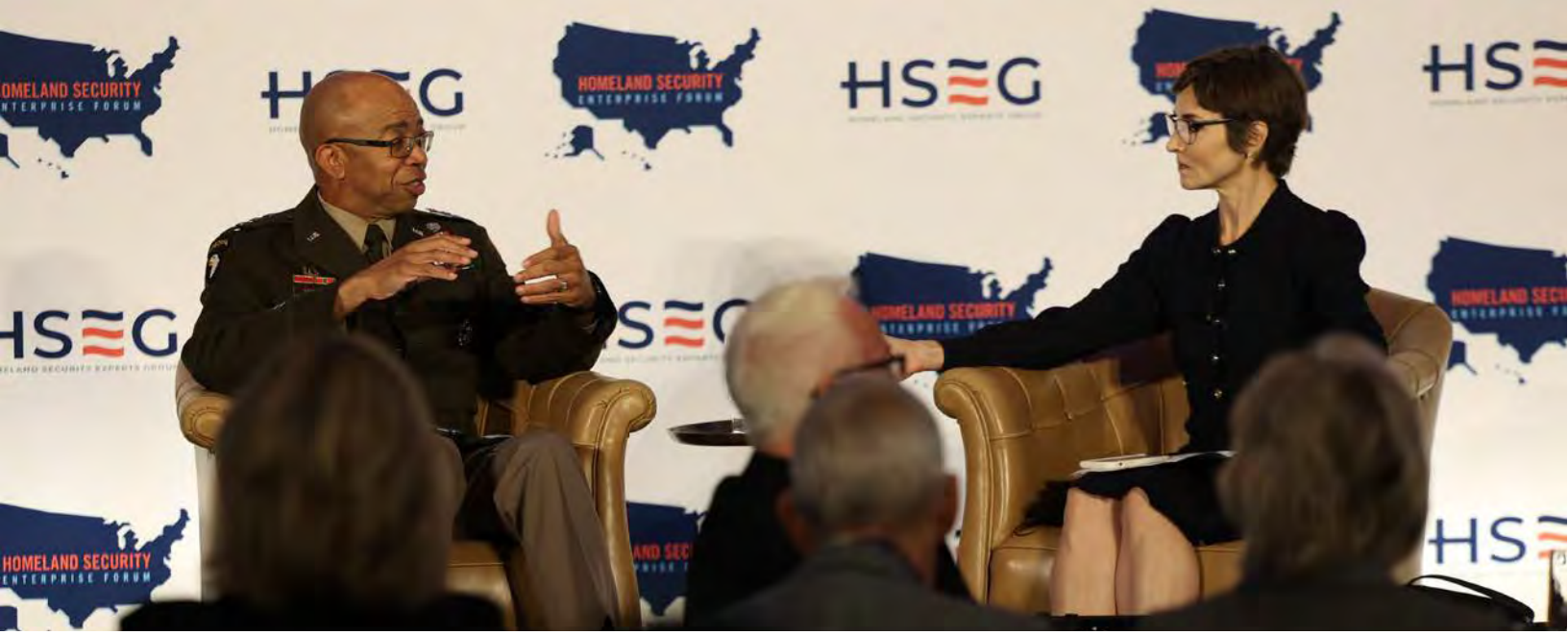
The threat from small unmanned aerial systems (sUAS) has grown significantly over recent years. At one end, the ubiquity of off-the-shelf sUAS devices has resulted in increased instances of accidental trespasses into restricted airspace. At the other, sUAS pose significant threats in narcotics trafficking, espionage, carrying and deploying weapons and explosives, and other criminal behaviors.

While the need is urgent, the roles and responsibilities associated with countering sUAS (CUAS) is currently piecemeal. Participants echoed concerns about both policy and mitigation authorities, noting a lack of clarity has led to significant delays in the development and deployment of technology to mitigate threats. There was consensus from participants that even if the authority to operate CUAS is clarified in legislation, many airports and critical infrastructure organizations may be unable to procure and deploy the technology immediately due to budget cycle restrictions. To address this timing gap, and incentivize industry to address the larger security gap, participants discussed the provision of grants or other federal funding opportunities to help support CUAS procurements, as a viable solution.

Participants also discussed the challenges associated with effectively quantifying and publicly describing the threat as it continues to evolve. Participants specifically acknowledged that because a large portion of the sUAS in use and being sold in the US are produced by an adversary nation, the US risks additional threats it is not effectively positioned to counter. They also noted the need to continue to advance efforts under the Domestic Counter-Unmanned Aircraft Systems National Action Plan and through other opportunities now under current authorities and continuing to gather empirical data to support advancing the legislative agenda.

COUNTERING UNMANNED AERIAL SYSTEMS RECOMMENDATIONS:

- **Build budget proposals that enable federal agencies to address the threat and advocate for progress, rather than waiting for the legislative environment to be resolved before investing. These budget proposals can be drafted to reflect work that should occur in the absence of updated legislation, as well as a version should the legislation pass.**
- **Focus on communications. Develop awareness, campaigns, and education to explain the current threat and risk environment. Identify ways to educate the public and press legislators to address the growing threat. Continue to engage privacy advocacy groups, and other key stakeholders on the technology involved, as well as procedures, governance, and processes that would be used to counter UAS. Build a bigger constituency through exercises. Leverage subject matter experts—including former government leaders—to talk to the appropriate stakeholders. CUAS policy that provides clarity on operational control in the case of threat and creates grant opportunities for private sector aviation and other critical infrastructure organizations to procure tested technologies is needed in the immediate short term.**
- **Engage Congress and the Presidential Administration to highlight the time-sensitive nature of this threat and the industry's need for clarity on operational authority to begin developing mitigation procedures.**



MATURING THE HOMELAND ENTERPRISE

The maturation and evolution of the threat facing the United States necessitates a similar maturation of the homeland security enterprise. Participants highlighted that a successful national security strategy needs to include all-domain awareness, clear roles and responsibilities, and new ways of thinking about short- and long-term solutions to the varied threats. Participants repeatedly acknowledged that the United States cannot continue to measure its success solely because there has not been an international terrorist attack since September 11, 2001. The homeland enterprise has made significant progress in the last 20 years; but more is needed.

Participants highlighted the continued need to partner across the federal government and between the federal government and stakeholders, including the private sector, and FFRDCs, to prepare for, respond to, and recover from national security emergencies. Participants agreed that preparing for, responding to, and recovering from national security emergencies requires appropriated and allocated resources and acknowledged there will not be enough resources to support the entire nation, so deliberate partnerships in constructing and exercising plans and strategies are needed to ameliorate the impacts. Participants repeatedly acknowledged the importance and efficacy of engagement between government, private sector, and critical infrastructure owners and operators on current and emerging threats and opportunities to effectively respond.

Partnerships were also identified as an important mechanism to facilitate innovative and collaborative research, leverage promising practices and lessons learned from international stakeholders, and strengthen preparedness; ensure understanding of threats—particularly in the cyberspace—and have businesses and governments identify mutually-beneficial structures and policies; and continue to identify, collect, and share data. Participants stressed the need to continue exercising together, meeting and pursuing campaigns day-to-day, to show our capacity and will to work and learn together. The suggestion that we continue implementing the successes of the JTTF model to cyber was also made and supported by participants.

As the conversations delved further into data, participants noted the importance of identifying, collecting, sharing, and leveraging the appropriate data to rapidly develop options, collaborate with allies and partners, and create meaningful solutions. The promising strategy identified centered on integrated deterrence. Four principles govern this approach: 1) domain awareness (how do you sense and detect the issues through data); 2) information dominance (how do you take the data and make sense of it faster, so you have decision timeliness and decision priority); 3) decision superiority; and 4), global integration. It was explained that expedited data collection and understanding leads to

decision superiority—the ability to develop other options, collaborate with allies and partners, and create peaceful solutions. Participants identified partnerships related to data collection and understanding as the key to all-domain awareness.

Participants also identified data as foundational for establishing intelligent policies and governance structures. Participants discussed that the priority for the government is data standards and stressed the importance of guiding principles developed by private industry and other stakeholders to inform feasibility. Industry participants supported this by noting the need for government to provide direction on standards to use for different types of technologies and systems. Together, attention was also paid to the need for government and private stakeholders to partner in the development of on-the-job training in the evolving technologies and systems that are being used and projected to collect data and inform solutions, and to create career paths that encourage continued growth and development in key areas.

MATURING THE HOMELAND ENTERPRISE RECOMMENDATIONS:

- **Change the way we think, respond, and leverage technology. With the diverse array of threats we face, including cyber, economic vitality, theft of data, transnational criminal organizations, lone wolves, increasing challenges at our borders, and workplace violence, using the same processes we have used historically will leave us vulnerable. We must adapt information sharing processes and protections to effectively meet the demands of today, ensuring we address the need, level, and speed at which we share information.**
- **Advocate for updating the Privacy Act of 1974 to better align and work with the current technology environment. DHS should work with Congress to ensure US legislation takes into account legislation from other nations to provide an interoperable model for the private sector, where possible.**
- **Support the CDO Council and its activities to develop rich data catalogs that describe data assets, while recognizing that 100% is not an achievable goal. Focus on the highest value datasets that are in demand across the Homeland Security Enterprise, and work to ensure these assets are accessible to the extent practicable by law and within civil rights/liberties.**
- **Continue to invest in governance, streamlining current efforts, and making them both effective and efficient.**
- **Leverage the increasing relevance of FISA Section 702 in cybersecurity as a critical reason for its renewal, in addition to the existing foreign intelligence collection equities.**
- **Engage the private sector partners most vulnerable if 702 were not renewed in discussions with legislators. A decrease in collection capacity would not just make the government vulnerable, but high-value American business targets vulnerable as well, especially in the cyber domain.**

FUTURE OF THE MISSION SPACE

In recent years, the United States has seen a significant increase in the amount of goods crossing our borders, people moving through our transportation hubs, and threats and natural disasters impacting the homeland. A common theme in conversations held on the future of the mission space was the need for technological innovation and partnerships with whole-of-society stakeholders to address risks while enhancing movement of goods and people and the resiliency of communities. Participants agreed that in the ever-changing threat landscape characterizing the US, a proactive and innovative approach to identifying challenges and solutions remains key and the government cannot accomplish this task alone. The future of the mission space conversations explored and provided recommendations to the current issues in trade, travel, and disaster resilience.

TRADE

Cross-border trade is a critical economic driver for the United States. Since the start of the pandemic, it has grown more complicated, given the significant increases in the volume of goods, supply chain disruptions, and the prevalence of illegal substances making their way across the border. Outdated infrastructure, staffing shortages, and the sheer volume of trade has made it increasingly difficult for federal agencies, owner/operators, and industry to manage economic and national security needs at the border.

One of the major takeaways from this discussion was the need for technological innovation to address outdated systems, infrastructure, and threat concerns. Transportation hubs have successfully used technology like facial matching, artificial intelligence, automated threat recognition and data analysis to expedite the processing of travelers. Participants concurred federal agencies at the boarder could leverage the same approaches advancing these technologies to help expedite cargo processing times and improve security.

Implementing new technology and updating infrastructure underscores the need for a workforce with an understanding of these new systems. The group agreed that organizations should take new considerations into account when it comes to labor skill availability. The need to hire employees that can be trained across multiple systems and sets of equipment in order to expedite processing times while maintaining secure environments remains imperative.

Participants also agreed that partnerships across every level of the government, the private sector, and law enforcement are necessary. By working together, ports of entry will be better equipped with resources and updated infrastructure, and technological innovation can be leveraged to facilitate more efficient systems and improve security measures.

FUTURE OF TRADE RECOMMENDATIONS:

- **Continue to leverage partnerships between federal, state, local, and specialized law enforcement at ports, airports, and borders by dedicating resources and personnel to expedite inspections while ensuring cargo security.**
- **Consolidate and publicly release information outlining technological and infrastructural needs, along with the threat consequences, to drive joint investment and alternate business models with partners.**
- **Drive data integration to facilitate the use of AI for automated threat recognition and enhanced risk management, consolidated for a true operational picture.**
- **Empower effective strategies for infrastructure and technology acquisition by selectively incorporating multiyear funding into the OFO budget.**
- **Consider alternate career development paths and hiring processes to shorten the time to add new law enforcement personnel to the workforce.**

TRAVEL

Upgrading airport technology and security are key elements at the forefront of the future of travel. With travel reaching levels commensurate with pre-pandemic, accompanied by an increase in airport staff shortages, technology innovation remains critical to enhance both the customer travel experience and airport/air security. Currently, TSA officers make 30% less than colleagues in similar federal positions. Pay parity and pay equity is critically important to ensuring TSA's ability to recruit and retain a highly qualified workforce who can implement and deploy emerging technological solutions.

Participants discussed that DHS has made substantial strides in its implementation of biometrics supporting border security and facilitation missions. DHS deployed Simplified Arrival rapidly for international inbound travelers and increasingly for the outbound persons, and innovative pilots have been run by numerous private sector organizations in coordination with TSA. Discussions also focused on the successful and complete

implementation of biometrics into the CBP and TSA international missions, while noting the importance of privacy, civil rights and civil liberties, and trust in government and business stakeholders to use biometrics appropriately.

Another topic of discussion was the concept of Open Architecture as a technological solution to meet global security mandates, enhance passenger facilitation goals of speed/convenience, and address long-term operational fallout from COVID-19. Participants discussed that DHS should examine how to partner with private sector entities to provide data that can be used to enhance the training of algorithms related to developing efficiencies in travel, while protecting privacy and civil liberties and maintaining strong controls over the data.

Similar to other areas, participants identified partnerships as a fundamental component of addressing the future of travel. Strong partnerships can help airports allocate resources properly, share the necessary data to increase security, and implement promising practices of others to better our systems and processes. Participants in the travel sessions discussed new solutions like OneStop security that aims to make traveling more efficient, strengthen partnerships with other governments, and make travel more secure by implementing US screening services on flights inbound to the US.

FUTURE OF TRAVEL RECOMMENDATIONS:

- **Promote passage of legislation advancing pay parity / pay equity for TSA employees, to ensure they are paid commensurate to their federal counterparts, and "OneStop" security which would allow passengers and baggage arriving on inbound flights to the US to bypass additional security checkpoints if they've been screened by TSA-comparable security measures prior to arriving.**
- **Support the rapid incorporation of Open Architecture, or standards for how data must be made available from CT or other screening equipment, in US markets, and advocate for its adoption globally – particularly in markets with significant US-bound travel.**
- **Advocate for the incorporation of biometrics into the international border and travel ecosystem, including at land and maritime ports of entry. Recommending ways in which DHS can better communicate to the public about the use of biometrics and protections for travelers and transportation workers.**
- **Engage government entities, such as DHS Privacy and CRCL, as well as their private sector advisory committees, to highlight the importance of privacy and civil liberties representatives being seen as leaders in the implementation of emerging technology within the domestic and international travel ecosystem.**
- **Engage in policy conversations with DHS-adjacent industries such as aviation and travel to help set foundational privacy and civil liberties standards for the exploration and implementation of emerging technologies such as Open Architecture, Biometrics, and CUAS.**

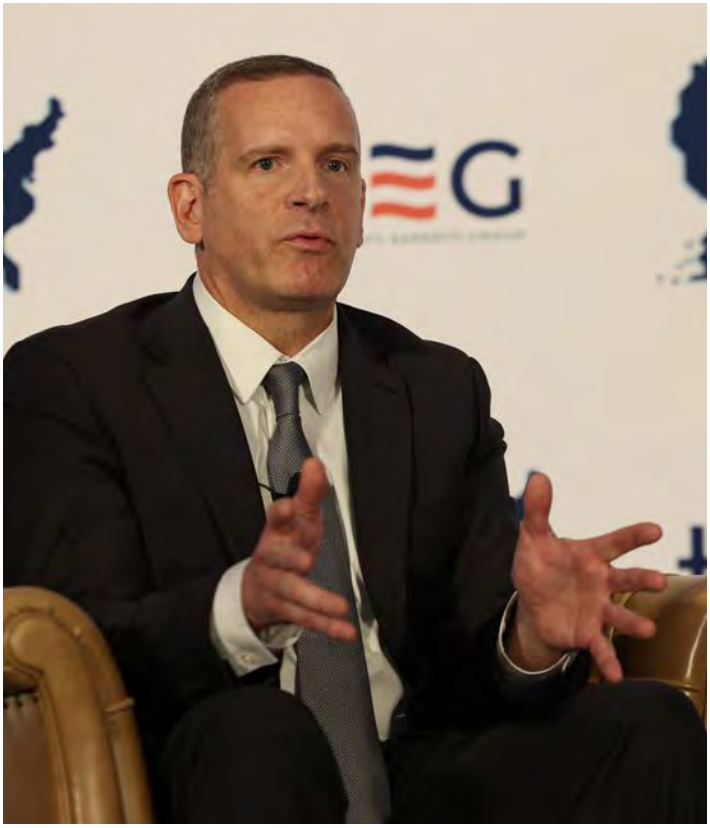
RESILIENCE

Resilience applies across the homeland security enterprise. As threats continue to emerge and re-emerge, withstanding threats and recovering quickly has never been more relevant.

Conversations about resiliency focused specifically on reducing disaster risks and addressing threats of mis-, dis-, and mal-information. Participants underscored the need for the United States proactively address threats, noting that complacency is the antithesis of resilience. There was consensus that embracing agile methods of response and locally resourcing needs to respond to emergencies faster exists as one of the drivers of a more resilient nation.

Participants agreed about the need for stronger partnerships between the government and the private sector. They noted that the federal government alone cannot achieve resilience and advocated for better ways to incentivize resilience actions to reduce risks. This includes investments in preparedness, hazard mitigation, and insurance, and collaboration from the finance, insurance, and real estate industries.

Participants also highlighted partnerships as a solution to addressing threats of mis-, dis-, and mal-information. When the government, media, private sector, and communities work together on joint messaging and



communications, they can play an important role in providing accurate, transparent information and addressing inaccuracies.

The group strongly agreed that in the current threat environment we face, risks need to be proactively identified and jointly addressed among partners. No one actor can tackle these issues alone.

RESILIENCE RECOMMENDATIONS:

- **Incentivize resilience actions to reduce the risks the nation faces. This requires partnerships between the public and private sectors, including the finance, insurance, and real estate industries.**
- **Countering mis-, dis-, and mal-information requires partnerships between the government, business, media, and communities. Left unaddressed, mis-, dis-, and mal-information can cause harm to disaster survivors and create distrust between stakeholders.**

CONCLUSION

Subject matter experts from the public and private sector openly exchanged ideas and recommendations related to identifying and mitigating emergent manmade and natural disasters and threats, maturing the homeland enterprise to reduce the nation's risks, and the future of the mission space. The takeaways and recommendations provide clear direction for the Homeland Security Experts Group and HSEF attendees to act on, and partnerships to build and enhance. As was highlighted throughout the Forum, the key to facing the evolving and maturing threats facing the US is the ability for subject matter experts across sectors to partner, collaborate, and have open and honest conversations about the challenges and potential solutions. The Homeland Security Experts Group will continue to facilitate these partnerships and conversations and lead engagements focused on implementing the recommendations and ensuring solutions to our greatest challenges: respecting our fundamental national traditions, Constitutional rights, and continuing to contribute to the safety, security, prosperity, and resilience of our nation.

CORPORATE PARTNERS

The private sector plays a critical role in providing solutions to the mission space. Their support and feedback at the forum helped make the recommendations in this report further more attainable. We would like to recognize our incredible partners:

PRESENTING SPONSOR

MITRE

PLATINUM SPONSOR

intelligence² DEBATES

GOLD SPONSORS

American Airlines

CLEAR

Guidehouse

Peraton

SILVER SPONSORS

aws

CORNERSTONE AN EMPLOYEE-OWNED COMPANY

Clarivate™

Google

Hidden Level

INFRAGARD NATIONAL MEMBERS ALLIANCE

LOCKHEED MARTIN

Microsoft Federal

PANGIAM

S2 GLOBAL An OSI Systems Company

SAIC

BRONZE SPONSORS

accrete ai government

GDIT

SEVTECH

SIMS SOFTWARE

smiths detection

UNITED AIRLINES

WHITNEY STRATEGIC SERVICES

SMALL BUSINESS SPONSORS

Airlines for America We Connect the World

GOST Powered by Giant Oak

INSTABASE

Logically.

SAVE THE DATE

THIRD ANNUAL

HOMELAND SECURITY ENTERPRISE FORUM

NOVEMBER 6-8, 2023

SALAMANDER RESORT | MIDDLEBURG, VA

Email: info@homelandexperts.org
Website: hsenterpriseforum.com