



# Homeland Security Advisory Council

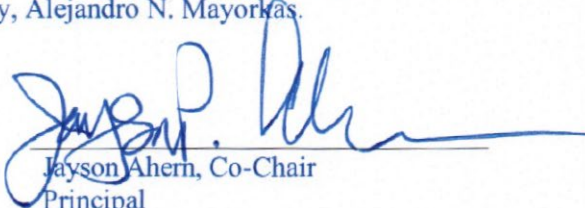
Intelligence and Information Sharing  
Final Report

March 16, 2023

This publication is presented on behalf of the Homeland Security Advisory Council, Intelligence and Information Sharing Subcommittee, Co-Chaired by Vincent Talucci and Jayson Ahern to the Secretary of the Department of Homeland Security, Alejandro N. Mayorkas.



Vincent Talucci, Co-Chair  
Executive Director & CEO  
International Association of Chiefs of Police



Jayson Ahern, Co-Chair  
Principal  
The Chertoff Group

This page is intentionally left blank.

## TABLE OF CONTENTS

---

INTELLIGENCE AND INFORMATION SHARING SUBCOMMITTEE	5
HOMELAND SECURITY ADVISORY COUNCIL STAFF	5
EXECUTIVE SUMMARY	6
METHODOLOGY	7
RECOMMENDATIONS	7
CONCLUSION	12
APPENDIX 1: TASKING LETTER	13
APPENDIX 2: SUBJECT MATTER EXPERTS AND OTHER WITNESSES	19
APPENDIX 3: GLOSSARY	22

## **INTELLIGENCE AND INFORMATION SHARING SUBCOMMITTEE MEMBERS**

---

<b>Vincent Talucci, Co-Chair</b>	<b>Executive Director &amp; CEO International Association of Chiefs of Police (IACP)</b>
<b>Jayson Ahern, Co-Chair</b>	<b>Principal The Chertoff Group</b>
<b>Lynda Williams</b>	<b>Professor of the Practice Middle Tennessee State University</b>
<b>Jonathan Thompson</b>	<b>Executive Director &amp; CEO National Sheriffs' Association</b>
<b>Ali Soufan</b>	<b>Chairman &amp; CEO The Soufan Group, LLC</b>
<b>Michael Masters</b>	<b>National Director &amp; CEO Secure Community Network</b>
<b>William Bratton</b>	<b>Executive Chairman Teneo Security Risk Advisory</b>
<b>Patrick Yoes</b>	<b>National President Fraternal Order of Police</b>
<b>Courtney Adante</b>	<b>President Teneo Security Risk Advisory</b>
<b>Kerry Sleeper</b>	<b>Senior Advisor Secure Community Network</b>
<b>Gene Voegtlin</b>	<b>Director, Policy and Governance International Association of Chiefs of Police</b>

## **HOMELAND SECURITY ADVISORY COUNCIL STAFF**

---

<b>Rebecca Kagan Sternhell</b>	<b>Executive Director</b>
<b>Alexander Jacobs</b>	<b>Senior Director</b>
<b>Joseph Chilbert</b>	<b>Senior Director</b>
<b>Carley Bennet</b>	<b>Intern</b>

## EXECUTIVE SUMMARY

---

Following the September 11<sup>th</sup>, 2001 terrorist attacks against the United States, federal, state, local, tribal, and territorial partners gathered to design a domestic information sharing infrastructure to enable the rapid and continuous exchange of information to identify and eradicate terrorist threats. Since then, the Department of Homeland Security has improved its processes to combat an expanding range of threats to domestic security.

In October 2022, the Secretary of Homeland Security tasked the Homeland Security Advisory Council (HSAC) to form a subcommittee on Intelligence and Information Sharing to develop recommendations on how the Department can improve its intelligence and information sharing with key federal, State, Local, Tribal, Territorial and Campus (SLTTC), and private sector partners. The Secretary requested advice and recommendations to better enable DHS Intelligence and Analysis (I&A) to efficiently share information and intelligence with key partners. In particular, the Secretary set the following tasking:

1. Recommendations for how the Department can rapidly and efficiently share intelligence and information with its federal, SLTTC, and private sector partners, considering if DHS investments in information sharing technology and changes in law and policy have resulted in increased knowledge transfer and resilience and if further investments or changes in law or policy are needed.
2. Recommendations on enhancing DHS' information and intelligence sharing architecture to better spread knowledge and swiftly share critical information, through assessing current capabilities and steps for improvement.
3. Recommendations on how to position the current DHS information sharing architecture to optimize its information sharing for threats other than terrorism, for example: cyber, border security, foreign influence/propaganda, strategic advantage, and others.
4. Recommendations on internal DHS information sharing and how well DHS has implemented its internal information sharing policies, such as the One DHS Memo, so that the Department can leverage DHS data and information to support its missions, like border security, as well as develop and share relevant, quality intelligence with partners.

Since November 2022, the Subcommittee met with leaders and subject matter experts from the Department, other federal entities, and a variety of state and local law enforcement. Consistent themes emerged from the briefings and roundtable, with input from a wide range of invested parties – the need for a feedback mechanism loop from the local officer to the federal agent, enhancing the utility of a shared database that is open and easily accessible to all levels of law enforcement and intelligence, and improving the collaboration between DHS and Department of Justice in interdicting and preventing illicit activities.

Recognizing that I&A operates in a dynamic and ever-changing environment, it is not possible to address every issue in a static, time bound report. The Subcommittee focused its work on addressing fundamental and systemic concerns that have been, or could be, viewed as limiting the effectiveness

and capabilities of I&A and its value to its partners in SLTT. To that end, this report presents several specific recommendations that the Subcommittee believe can help DHS improve intelligence and information sharing with law enforcement partners.

## **METHODOLOGY**

---

The Subcommittee drew upon expert interviews and supplemental research from November 2022 to February 2023. Specifically, the Subcommittee met with representatives, subject matter experts, and leaders from DHS I&A, U.S Customs and Border Protection (CBP), the National Counterterrorism Center, the Cybersecurity and Infrastructure Security Agency (CISA), and the Criminal Intelligence Coordinating Council (CICC).

The Subcommittee also felt it imperative to talk to state and local law enforcement, as they are the end-users of DHS intelligence and information products. To accomplish this, the Subcommittee first held a roundtable with representatives and leaders from Fraternal Order of Police, the International Association of Chiefs of Police, and the National Sheriffs' Association. The Subcommittee also met with regional law enforcement divisions from northern Texas and New York state. These groups utilize Fusion Centers and were able to speak to DHS products and their engagement in intelligence and information sharing.

Additionally, the Subcommittee reviewed recommendations proposed during the 2022 Intelligence Summit hosted by IACP, DHS, and other national law enforcement organizations. The Subcommittee sought to tailor the Intelligence Summits' recommendations to DHS by focusing on its organizational structure and its products delivered to DHS partners. Based on expert input, supplemental research, and insight from the intelligence community, the Subcommittee identified substantive and meaningful recommendations to support and enhance the Department's information and intelligence sharing efforts with its partners. The Secretary acknowledged and endorsed the summit's recommendations as the cornerstone for reaffirming DHS's support and commitment to work diligently with the law enforcement partners to implement the recommendations.

## **RECOMMENDATIONS**

---

While significant work has been done, both from DHS and I&A, the ever-changing threat landscape necessitates the continued pursuit of improvement. Through the Subcommittee's investigation, they've identified several key findings derived from overarching themes.

Key themes included: the need to maximize and capitalize on existing, critical opportunities; the need to embrace nimbleness to adapt quickly to a changing, dynamic threat environment; the need to assess and bolster today's technology solutions ensuring seamless sharing and virtually binds key stakeholders; and the need to invest in, and in some cases reinvigorate, infrastructure at all levels of the enterprise.

The recommendations put forth in this report are broad so as to provide a wide berth for the Secretary to identify appropriate policy and operational responses. The Subcommittee worked to identify areas

for improvement and offers practical and well-resourced recommendations to help improve information and intelligence sharing and prevent any future strategic surprise. This can be achieved by harmonizing federal, state, local, and tribal lines of effort to collect, conduct, and disseminate actionable intelligence throughout the various agencies and departments.

The following recommendations are made via the Subcommittee's assessment of potential agency enhancements across the enterprise, to include increased connectivity with state, local, tribal, and federal law enforcement. Notably, the below recommendations, contextualized from the key findings and focused largely on infrastructure and provision of potential support from I&A, parallel recommendations offered in the most recent Intelligence Summit report.

**Key Finding #1 The need for DHS to maximize and capitalize on existing critical opportunities.**

**Recommendation:**

The Subcommittee recognizes and appreciates the Department's effort to reflect on its own performance and identify areas for improvement. Complementing the present intelligence and information sharing (IIS) efforts, DHS recently partnered with key state, local, tribal, and federal stakeholders to produce the *2022 Intelligence Summit: Information Sharing in a Dynamic and Evolving Threat Environment*. To capitalize on this comprehensive report, and to avoid duplication of efforts, the Subcommittee recommend DHS adopt and work to fully implement the recommendations contained within the January 2023 Final Report<sup>1</sup>.

The 2022 Summit was organized into six focus areas with opportunities for participants to provide insight and feedback. Key findings and recommendations were identified aligned to the following consistent themes:

1. The critical importance of broadly sharing intelligence in a timely manner and at the lowest classification level possible during times of steady state and in response to critical incidents.
2. The necessity to fully embrace the leading role that the Criminal Intelligence Coordinating Council (CICC), as part of the Global Justice Information Sharing Initiative (Global) Advisory Committee (GAC), must play in supporting and coordinating efforts across all levels of government to develop and share criminal intelligence and information across the nation.
3. The need to identify and address diverse training gaps that impact all levels of law enforcement. This includes seeking out opportunities to reenergize and enhance the identification and reporting of suspicious activity for all national security threats through the Nationwide Suspicious Activity Reporting Initiative.
4. Recognizing, and supporting, the vital role that SLTT law enforcement intelligence fusion centers, real time crime centers, and/or other criminal information sharing networks or organizations play in enabling information sharing that is vital to national security. This includes the need for federal partners, specifically the Federal Bureau of Investigation (FBI) and DHS Office of Intelligence and Analysis, to assign personnel to all state and major urban area fusion centers to further enhance connectivity and information sharing.

---

<sup>1</sup> Available at [https://www.theiacp.org/sites/default/files/2022\\_Intelligence\\_Summit\\_Post-Event\\_Report.pdf](https://www.theiacp.org/sites/default/files/2022_Intelligence_Summit_Post-Event_Report.pdf), March 9, 2023



5. The necessity of ensuring strong protections of privacy, civil rights, and civil liberties across all intelligence and information sharing efforts.

**Key Finding #2 The need for DHS to embrace nimbleness to adapt quickly to a changing, dynamic threat environment.**

**Recommendations:**

1. DHS should reaffirm in clear policy, and as part of the “DHS Strategic Framework for Countering Terrorism and Targeted Violence,” the following vision statement that was called for but never implemented:

“The Department will collaborate with SLTT partners to share developed intelligence and enhance analytic and information-sharing process, with a focus on standardizing product and reporting processes and dissemination mechanisms across the DHS Intelligence enterprise. The Department will initiate a shared services program to facilitate common processes for managing production, reporting dissemination, tracking, and providing feedback on products and reports across the entire DHS Intelligence enterprise. This effort will help SLTT partners have relevant and actionable information.”
2. The Department should explore opportunities to reenergize and enhance the identification and reporting of suspicious activity for all national security threats through the Nationwide Suspicious Activity Reporting Initiative. Given the collaborative nature of this space, such efforts should include an external facing outreach and engagement effort with key stakeholders.
3. The Department and its Office of State and Local Law Enforcement should address and prioritize a better outreach and information flow to smaller agencies that lack the capacity and resources to be privy to intelligence information in real time.
  - a. Based on feedback, access to a particular website or dial-in on a secured line in which information can be received in a timely manner is something that would be welcomed by SLTTC.
  - b. Additionally, to further strengthen the relationships with large and small SLTTC, the Subcommittee recommends the Department make available the appropriate number of I&A Analysts in each fusion center, Joint Terrorist Task Forces (JTTF), major city police intelligence and other entities as determined by I&A.
  - c. Small police agencies, and the governments that oversee them, often do not have vetted government email addresses. DHS should explore an outreach network that can delve into even the smallest of communities and encourage that community to participate in the country’s intelligence initiatives.
4. Additional study needs to be conducted on how to streamline information dissemination to public sector partners who also happen to be foreign operators (e.g., a vessel or terminal

operator managing facilities within a US port). Based on conversations with partners and fellow HSAC Subcommittees, the Subcommittee found that the private sector plays an important role in timely information and intelligence sharing, and that the Department can find additional ways to share information to increase security.

5. Over-Classification. Scaling down classification / Scaling up access
  - a. Often, information is over-classified and should be de-classified, when possible, for better dissemination to core partners. I&A should look to de-classify information wherever feasible to better inform and equip partners.
  - b. I&A should consider increasing the number of security clearances for SLTTC to ensure that those who need information have the ability and capability to access it in a timely fashion.
6. The Department should continue improving intelligence and information dissemination efforts to State, Local, Tribal, Territorial, and Campus Law enforcement. In discussions, it became clear that, while DHS does seek to share information with SLTTC partners, its efforts are often highly segmented which can lead to multiple calls, meetings, briefings in a short timeframe which places a strain on the resources of SLTTC agencies. The volume of this information and the lack of a unified distribution approach severely strains the ability of SLTTC agencies to effectively process the information, which in turn may leave them unclear or unprepared to act on the information appropriately. A related challenge identified was the urgent need for better coordination between federal entities, primarily the Department of Justice and the Department of Homeland Security to avoid overlap and minimize confusion for SLTTC Partners.
  - a. DHS should establish a more unified, enterprise-wide approach to intelligence/information sharing and collections requirements. This begins with clear policy and guidance that defines roles and responsibilities, as well as a structural architecture for all department-level entities, as well as components, to include a Governance structure to oversee its implementation and functioning. This recommendation is not limited only to the Department sharing information, but also to reporting and collections requirements as well.
  - b. I&A, working with other DHS components like OPE and CISA, should develop a written protocol intended for dissemination to SLTTC partners. The protocol should clearly outline and set expectations for the type of information, response, or other materials or assistance that they will receive from I&A when addressing a threat with nation-wide implications or following a critical incident.
  - c. I&A should ensure they have the policy, guidance, and tools in place to offer timely calls and intelligence products in the event of a rapidly developing threat scenario that has nation-wide implications. Stakeholder feedback revealed that oftentimes information came after an incident or event, rendering it effectively moot. Additionally, information was distributed by multiple federal departments, and often distributed by

multiple offices within those departments, resulting in information overload and confusion on behalf of the recipients.

**Key Finding #3 The need to assess, and bolster, today’s technology solutions that help enhance seamless sharing and virtually binds key stakeholders.**

**Recommendations:**

Significant work remains in developing, establishing, and deploying a system that will allow for the timely convening of law enforcement agencies nationwide in times of crisis to better share actionable and relevant threat information.

1. The Department should identify and codify the common federal and SLTTC mechanisms and systems utilized for disseminating intelligence products, threat notifications, and information, with an emphasis on mobile applications that allow secure and real-time information sharing across the sworn and non-sworn law enforcement community.
2. The Department should consult with fellow federal partners to avoid the creation of stove-piped and competing platforms and apps for sharing threat information and intelligence products. By integrating efforts through a collaborative approach, the federal government should create efficiencies and avoid duplication of effort.
3. The Department should work with SLTTC law enforcement associations to develop a consistent, user-friendly mechanism/platform for managing and promoting information sharing during times of steady state (strategic) and in response to critical incidents (tactical). This effort should include identifying and codifying the thresholds and criteria for SLTTC-led and integrated SLTTC partners’ participation in planning and executing national calls in response to critical incidents.

**Key Finding #4 The need to invest, and in some cases reinvigorate, infrastructure at all levels of the enterprise.**

**Recommendations:**

There is a need to reinvigorate or reimagine a central coordinating body to organize and make information and intelligence sharing more effective at the Federal level, which includes the Departments of Defense, Justice, and Homeland Security. This effort should be coordinated closely between the Departments.

Whether a new model of cooperation is envisioned, or the reestablishment of the crucial role that the Program Manager for the Information Sharing Environment (PM-ISE) once had, this coordinated approach and “one stop shop” to synchronize and share information at all levels of government is vital and necessary.

Streamlining policy and operational feedback to DHS, through working directly with state, local, and

tribal law enforcement leadership, via a refocused and appropriately resourced Criminal Intelligence Coordinating Council, will allow the Department to receive timely information and intelligence while providing the same in return.

The Subcommittee suggests the return to programmatic efforts focused on providing technical assistance to fusion centers so to enable a baseline capability, and so to ensure governance and policy consistency across and between fusion centers. Investments could include:

1. Developing a framework or “playbook” that can assist those establishing, or for recently established, fusion centers to encourage consistency and efficiency across the network.
2. Updating existing guidance to identify best-practice technology platforms and solutions for consideration by fusion center stakeholders, focused on integration.
3. Continuing to embed the appropriate level of I&A resources within fusion centers to ensure connectivity with state, local, and tribal law enforcement, the private sectors, and NGOs, to include faith-based groups and develop specific outreach and engagement plans for the same.

## CONCLUSION

---

As the Department of Homeland Security celebrates the 20<sup>th</sup> Anniversary, it is important to reflect on why the department was created, to safeguard the American people and protect the homeland. The youngest but third largest cabinet department, today DHS’s mission spans across terrorism prevention, law enforcement, immigration services, transportation security, emergency response and recovery, cybersecurity and so much more. The agencies and offices that comprise DHS are on the front lines of the most pressing challenges facing our nation’s security. In order for DHS to most effectively execute its many missions, it is essential to fully engage the country’s state, local, tribal, territorial, and campus law enforcement agencies as a force multiplier. To achieve optimal effectiveness, it begins with the efficient flow of information and intelligence to those who need it for public and officer safety.

It is the collective opinion of the Subcommittee that DHS I&A has done a very good job of advancing the culture of sharing intelligence but certainly more can always be done. This Subcommittee focused on the actions it deemed critical to advance this challenge and provide the Secretary and Undersecretary I&A, with doable recommendations that the Subcommittee strongly believe will result in stronger security of the homeland through an enhanced structure of information sharing with its most critical partners in this undertaking.

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**

A handwritten signature in blue ink, appearing to read "Alejandro N. Mayorkas", is written over the typed name and title.

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 20<sup>th</sup> 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

<b>Name</b>	<b>Title</b>	<b>Organization</b>
Zack Beagle	Sergeant	DFW Airport Police Department, Fort Worth JTTF
David Berg	Assistant Director of Operations Support	National Counterterrorism Center
Stephen Biggs	Deputy Chief	Mesquite Police Department
Andrew Crowe	Lieutenant Colonel	Office of Counter Terrorism, New York State Police
Terrence Cunningham	Deputy Executive Director	International Association of Chiefs of Police
Lindsey DeBord	Deputy Director	North Texas Fusion Center
Stephanie Dobitsch	Deputy Under Secretary	DHS Office of Intelligence and Analysis
Kieran Donohue	Sheriff	Canyon County Sheriff's Office, Idaho
Ty Eanes	Deputy Executive Director	Border Security Intelligence Center
Michael Edgerton	Manager	Port Security, Port Authority of New York and New Jersey
Heather Fong	Assistant Secretary	Office of Secretary
Major Keith Golden	New York State Intelligence Center (NYSIC) Fusion Center Director	NYSIC

Zandreia Green	Associate Director	Cybersecurity and Infrastructure Security Agency (CISA) Intelligence, Integrated Operations Division, CISA
Terry Hastings	Senior Policy Advisor	Division of Homeland Security and Emergency Services, New York State
John Iorio	Executive Director	Office for State and Local Law Enforcement
Gina Jones	Department of Public Safety Regional Intelligence Supervisor	Intelligence and Counterintelligence Division North Region
Robert J. McConnell Jr	Captain	NYSIC, New York State Police
James Mandryck	Deputy Assistant Commissioner	U.S. Customs and Border Protection
Alberto Martinez	Director	Orange County Intelligence Assessment Center and Orange County Sheriff's Department
Malcolm McLaughlin	Director	North Texas Fusion Center
Mike Milstead	Vice Chair	US Attorney General's Global Advisory Committee and Member of National Sheriffs' Association
Erica O'Bryon	Lieutenant	Elm Ridge Police Department
Eric Peters	Deputy Director	U.S. Customs and Border Protection
Kevin Saupp	Counselor for National Security	Office of Intelligence and Analysis
Mike Sena	Chairman	Criminal Intelligence Coordinating Council (CICC)

James Smallwood	National Treasurer	Fraternal Order of Police
Ben Spear	Chief Information Security Officer	New York State Board of Elections
Keith Turney	National Sergeant-at-Arms	Fraternal Order of Police
Louis Torres	Department of Public Safety Regional Intelligence Supervisor	Intelligence and Counterintelligence Division North Region
Chad Quinlan	Deputy Director	Dallas Fusion Center
David Rausch	Vice President	International Association of Chiefs of Police
Ward Robinson	Director	Fort Worth Intelligence Exchange
Kenneth Wainstein	Under Secretary	Office of Intelligence and Analysis
Randy Watkins	Deputy Director	Fort Worth Intelligence Exchange
Jason Webb	Lieutenant	Dallas Sheriff Department
Stephen Williams	Director	Dallas Fusion Center
Michael Windham	Department of Public Safety Highway Patrol	Dallas District

## APPENDIX 3: GLOSSARY

<b>Term</b>	<b>Definition</b>
<b>CICC</b>	The Criminal Intelligence Coordinating Council supports state, local, and tribal law enforcement and homeland security agencies in their ability to develop and share criminal intelligence and information nationwide.
<b>CISA</b>	Cybersecurity and Infrastructure Security Agency, a DHS Component.
<b>Critical Infrastructure</b>	As defined in the U.S. PATRIOT Act so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.
<b>DOD</b>	Department of Defense
<b>DOJ</b>	Department of Justice
<b>FBI</b>	Federal Bureau of Investigation
<b>Fusion Centers</b>	State-owned and operated centers that serve as focal points in states and major urban areas for the receipt, analysis, gathering and sharing of threat-related information between State, Local, Tribal and Territorial (SLTTC), federal and private sector partners.
<b>GAC</b>	The Global Justice Information Sharing Initiative (Global) Advisory Committee (GAC) is a Federal Advisory Committee to the U.S. Attorney General, providing recommendations on promising national information sharing policies, practices, and technologies to solve problems and improve justice.
<b>HSIN</b>	The Homeland Security Information Network (HSIN) is the Department of Homeland Security's official system for trusted sharing of Sensitive But Unclassified (SBU) information between federal, state, local, territorial, tribal, international, and private sector partners.
<b>ICE</b>	U.S. Immigration and Customs Enforcement
<b>I&amp;A</b>	The Department of Homeland Security Office of Intelligence & Analysis
<b>JTTFs</b>	The FBI's Joint Terrorism Task Forces are the nation's front line of defense against terrorism, both international and domestic. They are groups of highly trained, locally based, passionately committed investigators, analysts, linguists, and other specialists from dozens of U.S. law enforcement and intelligence agencies.

<b>OPE</b>	The Office of Partnership and Engagement (OPE) coordinates the Department of Homeland Security's outreach efforts with critical stakeholders nationwide, including state, local, tribal, territorial (SLTTC) governments, SLTTC elected officials, SLTTC law enforcement, the private sector, and colleges and universities, ensuring a unified approach to external engagement.
<b>PM-ISE</b>	Program Manager for the Information Sharing Environment
<b>SLTT</b>	State, Local, Tribal and Territorial
<b>SLTTC</b>	State, Local, Tribal, Territorial, and Campus