ACKNOWLEDGEMENTS

INSA appreciates the efforts of everyone who contributed to the research and production of this white paper:

**HOMELAND SECURITY INTELLIGENCE COUNCIL**

Caryn Wagner, Chair
Barbara Alexander
George Bamford
Amy Choi
Andrew Coffey
Cindy Farkus
Dennis Hunt
George Jameson
Laura Manning Johnson
Elena Kim-Mitchell
Don Loren
Julie Nacos
Jordan Renga
Dawn Scalici
Judy Smith
Tony Spadaro
Jim Steiner
Don Van Duyn
Megan Woolsey

**INSA LEADERSHIP**

Letitia A. Long, Chairman
Chuck Alsup, President

**INSA STAFF**

Larry Hanauer, Vice President for Policy
Ryan Pretzer, Policy and Public Relations Manager
English Edwards, Marketing and Communications Manager
Joey Dahl, Intern
Aaron Lin, Intern
Christina Ma, Intern
Laura Wilkinson, Intern

**INSA SUPPORTS A HEALTHY PLANET**

INSA White Papers are printed on recycled paper that is 50% recycled content including 25% post consumer waste.
EXECUTIVE SUMMARY

The Homeland Enterprise consists of a vast series of formal and informal relationships between federal departments and agencies; state, local, tribal, and territorial (SLTT) entities; and the private sector. Each of these entities and relationships – some long established, others newly emergent – contribute to the body of information that is collected and analyzed to produce the intelligence necessary to protect the U.S. homeland. INSA’s Homeland Security Intelligence Council (HSIC) conducted interviews with more than 40 experts for their perspectives on the progress of the Enterprise and its remaining challenges 15 years after September 11, 2001, and five years after its first white paper on the topic. Forgoing a discussion of cyber threat intelligence and defense, this paper highlights four primary concerns highlighted by the interviewees:

1. The Office of Director of National Intelligence (ODNI) could have a clearer and more robust role as the coordinating body for homeland intelligence priorities and activities and the integration of homeland intelligence into national intelligence priorities and activities.

2. Interagency mechanisms that foster collaboration and information sharing amongst Enterprise partners offer best practices to work across the statutory and organizational boundaries and should be expanded and strengthened.

3. Information sharing efforts with SLTT entities would benefit from systematically informing them of current national priorities and information needs, streamlining the systems they use to receive federally-provided information, and providing a process and mechanism for them to share relevant information with federal partners.

4. Sharing government information with the private sector must now shift toward developing a truly reciprocal relationship, which requires the identification of sharing mechanisms that facilitate an interactive feedback loop between the government and the private sector and a more integrated government approach to meeting private sector requirements to protect critical infrastructure.

Paramount to each of these concerns is a need for solutions founded in the protection of civil liberties and privacy rights, and as appropriate, providing transparency that fosters the trust and cooperation of the public in this shared effort to protect the people, property and critical systems of the United States.
INTRODUCTION

The Intelligence and National Security Alliance (INSA) established the Homeland Security Intelligence Council (HSIC) in 2008 to promote understanding of the role of intelligence in the Homeland Enterprise (Enterprise), the successes it has achieved, and evolving challenges that continue to threaten our nation. The Enterprise consists of a vast series of formal and informal relationships between federal departments and agencies; state, local, tribal, and territorial (SLTT) entities; and the private sector. Each of these entities and relationships – some long established, others newly emergent – contribute to the body of information that is collected and analyzed to produce the intelligence necessary to protect the U.S. homeland.

In September 2011, INSA published an initial white paper on the topic, Intelligence to Protect the Homeland,\(^1\) which examined the Enterprise’s progress and leading challenges 10 years after 9/11. The paper offered 16 recommendations (see Appendix A) that were principally concerned with strengthening coordination, connectedness, and unity of effort across the Enterprise.

The 15th anniversary of 9/11 and the imminent election of a new president present a timely opportunity to reflect on years of evolving practice and revisit the paper, its recommendations, and the state of the Enterprise. Significant progress in areas like information sharing between federal and non-federal partners has been tested by evolving threats, particularly homegrown violent extremism inspired by the Islamic State (ISIS/ISIL) and other overseas extremist organizations. The activities of transnational criminal organizations and the ubiquity of threats from cyberspace have further blurred the boundaries between foreign and domestic threats and, as a result, between foreign intelligence and homeland intelligence. Integrating both types of intelligence within the Enterprise is essential to protecting the homeland and strengthening U.S. national security overall. INSA offers this paper as testament to the strides already made, and the challenges ahead, to enhance intelligence integration across the Enterprise.

\(^1\) Intelligence and National Security Alliance (INSA), Intelligence to Protect the Homeland: Taking Stock Ten Years Later and Looking Ahead, September 2011. At http://www.insaonline.org/i/d/a/b/Intelligence_to_Protect.aspx.
METHODOLOGY, DEFINITIONS, AND SCOPE

Using INSA’s 2011 recommendations as a guide, HSIC members interviewed more than 40 individuals with current or recent senior federal government experience within the intelligence and national security communities, in both policy making and operational roles. Perspectives from Capitol Hill, state and local agencies, the private sector, and nonpartisan research organizations also were represented in the interviews. HSIC members also consulted reports from within and out of government, notably those by Business Executives for National Security (BENS) in January 2015 and March 2016, respectively. HSIC members – many of whom served extensively at senior levels in the Enterprise – developed this white paper’s recommendations based on themes that emerged from the interviews and relevant literature.

Precise definitions have historically been a problem in discussing homeland intelligence. Consequently, interviews began with the respondents’ views of national intelligence as defined in the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004. Relating comments to this legal definition helped bound the discussion of homeland intelligence and how it fits into the larger legal framework.

National intelligence incorporates both foreign intelligence – collection and analysis activities directed toward foreign nations and organizations, foreign persons, or international terrorist activities that are conducted by one of the 17 elements of the Intelligence Community (IC) – and domestic intelligence, a term that is widely used but not defined in statute. Led by the Federal Bureau of Investigation (FBI), domestic intelligence targets threats to the United States from within its own borders. Law enforcement intelligence – information collected and/or analyzed by federal or SLTT law enforcement regarding criminal activity or other threats to the security of U.S. citizens, property and critical infrastructure – draws on different legal authorities to produce intelligence and information that can and should inform national intelligence.

“Integrating foreign and homeland intelligence within the Enterprise is essential to protecting the homeland and strengthening U.S. national security overall.”
HSIC’s definition of homeland security intelligence (which we now refer to as “homeland intelligence”) from INSA’s 2011 paper was “information that upon examination is determined to have value in assisting federal, state, local, and tribal and private sector decision makers in identifying or mitigating threats residing principally within U.S. borders.” Some interviewees contended the distinction of threats residing principally within the United States was unnecessarily narrow, since external threats to the homeland would also be considered homeland intelligence, but virtually all agreed that homeland intelligence was a subset of national intelligence and that it encompassed more than terrorism.

Homeland intelligence is most effective when it incorporates foreign and domestic intelligence and information from non-intelligence agencies that respond to the full range of national intelligence requirements. Not only is the Intelligence Community’s information useful to SLTT and private sector partners, but information from those partners can be useful to the IC on a variety of issues. The desired end state for the intelligence and law enforcement communities is to bridge the operational and statutorydivide in ways that respect each organization’s authorities and protect civil liberties while still delivering actionable intelligence to Enterprise customers.

Two assumptions were made to focus this paper and its recommendations:

1. As the statutory backbone of the Intelligence Community and intelligence activities in support of homeland security, the IRTPA was an extraordinarily complex piece of legislation. More than 10 years later, many observers would say it largely accomplished what it was designed to do. Although IRTPA may have shortcomings or have produced unintended consequences, Congress has shown little interest in undertaking additional broad reform efforts. INSA nonetheless strongly urges the incoming Administration and the next Congress to review IRTPA and other intelligence statutes, regulations, and guidelines for consistency and to clarify the roles, responsibilities, and authorities of the various elements of this complex architecture for homeland intelligence. Much of this clarification can be done within the executive branch, although some minor legislative changes may be required.

2. The cyber domain is an essential component of homeland security and homeland intelligence. It serves as an attack vector from which domestic and foreign adversaries can threaten utilities, financial systems, and other critical infrastructure sectors, as well as steal sensitive government, proprietary, and personal data. It is also the primary means of sharing information about cyber and non-cyber threats between Enterprise partners. Ensuring security of the cyber domain is of critical importance and immensely complex. Accordingly, cybersecurity as it relates to homeland security and the intelligence to support it demands a distinct evaluation and discussion, which is beyond the scope of this paper. This paper’s recommendations should be viewed as complementary to the numerous lines of efforts already under way to synthesize cyber threat information and share actionable cyber threat intelligence with partners across the Enterprise.
OPERATING ACROSS AUTHORITIES:
BRIDGING THE TITLE 50 DIVIDE

Many of the topics and concerns this paper addresses share an underlying dynamic—the need to operate effectively and legally across statutory boundaries between the activities of foreign-focused intelligence agencies and those of the more blended elements of the Homeland Enterprise. Because intelligence activities are governed by Title 50 of the U.S. Code, federal departments and agencies not explicitly charged with national security or intelligence missions are known as “Non-Title 50” partners. In the homeland sphere, maximizing information and intelligence integration requires a mix of traditional members of the national security community, such as the Department of Homeland Security’s (DHS) Office of Intelligence and Analysis (OIA), US Coast Guard Intelligence, and FBI; non-Title 50 components of DHS that possess security-related information, such as Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE); and representatives from other non-Title 50 organizations such as the Departments of Commerce, Transportation, and Health and Human Services (HHS). (See chart below.) To achieve fuller integration and coordination of homeland intelligence activities, interagency processes and mechanisms to help partners operate across these boundaries are increasingly necessary.

As the lines between foreign and domestic intelligence blur, and as it becomes clear that information gathered by law enforcement officials at all levels can be a critical piece of the overall intelligence threat picture, it is important to develop systems and processes to enable that sharing while preserving civil rights and liberties. Effective Homeland Intelligence will require leadership that can provide guidance for planning and coordination; mechanisms that offer meaningful, reciprocal and legal engagement amongst partners; channels that allow timely, two-way sharing of information; and training and oversight to ensure the protection of civil rights and civil liberties. The following sections will address each of these needs.

EXAMPLES OF TITLE 50 AND NON-TITLE 50 ENTITIES
Organizations with Title 50 intelligence authorities must work with a broad range of non-Title 50 partners, including other components of the same Federal agency.

<table>
<thead>
<tr>
<th>Examples of Title 50 Organizations</th>
<th>Examples of non-Title 50 Partners</th>
</tr>
</thead>
<tbody>
<tr>
<td>Central Intelligence Agency (CIA)</td>
<td>Centers for Disease Control (CDC)</td>
</tr>
<tr>
<td>Defense Intelligence Agency (DIA)</td>
<td>Department of Health &amp; Human Services (HHS)</td>
</tr>
<tr>
<td>National Security Agency (NSA)</td>
<td>Department of Transportation (DOT)</td>
</tr>
<tr>
<td>Department of State – Bureau of Intelligence and Research (INR)</td>
<td>Department of State – Rest of Department</td>
</tr>
<tr>
<td>Department of Treasury – Office of Intelligence and Analysis (OIA)</td>
<td>Department of Treasury – Rest of Department</td>
</tr>
<tr>
<td>Department of Homeland Security (DHS)</td>
<td>DHS – Rest of Department, including:</td>
</tr>
<tr>
<td>• Office of Intelligence and Analysis (OIA)</td>
<td>• Customs and Border Protection (CBP)</td>
</tr>
</tbody>
</table>

2“Non-Title 50” (NT-50) departments and agencies are those federal departments and agencies not listed as elements of the Intelligence Community (IC) in Title 50 of the United States Code or Executive Order 12333, United States Intelligence Activities (as amended July 30, 2008).
INCORPORATING THE HOMELAND INTO NATIONAL INTELLIGENCE PLANNING

Who should provide strategic leadership of homeland intelligence? Respondents expressed consensus (though not unanimity) that the Director of National Intelligence (DNI) should assume responsibility for this problem. No other official has the stature or the mandate to do so, and the role of the DNI is already one of coordination and integration of agencies with disparate authorities and missions. (It is important to note that we are not proposing the DNI in any way direct or task non-Title 50 organizations, but rather that he, his staff and elements of the IC work with them to develop systems and procedures to allow effective and appropriate partnership to take place.)

In 2004, the 9/11 Commission recommended introduction of a Deputy Director for Homeland Intelligence, reporting to the DNI. Congress did not implement this recommendation in IRTPA, nor did the ODNI create this position on its own, although some observers maintain that the proposal remains valid. BENS, for example, declared in its January 2015 report, “The absence of a designated domestic IC lead needs to be addressed.”

Even if future DNIs fail to create a deputy-level position, a requirement still exists for a focal point on the DNI staff with sufficient seniority to break down stovepipes and bring different constituencies to the table.

INSA believes an appropriately senior position on the ODNI staff would enable the ODNI to:

1. Set and prioritize requirements for homeland intelligence collection and analysis;
2. Ensure homeland intelligence requirements and products inform national intelligence efforts and objectives; and
3. Coordinate responsibilities for homeland intelligence activities so as to minimize duplication of effort and encourage each Enterprise member to operate within the full scope of its authorities.

---

Since 2011, the DNI has taken the first real steps to improve integration of homeland intelligence activities vis-à-vis the broader IC. A program first piloted in 2011 designates Special Agents in Charge (SACs) at a dozen key FBI field offices as “Domestic DNI Representatives,” charged with coordinating the efforts of Title 50 entities operating in the homeland in a manner similar to the role played by DNI Representatives and embassies and combatant commands. The DNI also broadened the charter of the National Intelligence Manager (NIM) for the Western Hemisphere to include a deputy focused on homeland intelligence. This step was a significant acknowledgement by the DNI that the IC had responsibilities and authorities regarding the homeland, albeit without the stature of a deputy DNI.

While these steps were positive, they were modest and must be built upon. INSA believes that the critical function of coordinating collection and analysis on threats to the homeland must be appropriately recognized and resourced. In the absence of a deputy DNI for the homeland, the DNI should appoint a separate NIM for the Homeland to serve as the focal point on the DNI Staff for Homeland Intelligence. Given the critical roles that DHS and FBI play in collecting and analyzing homeland intelligence, the DNI should consult closely with the DHS Under Secretary of Intelligence and Analysis and the FBI National Security Branch Executive Assistant Director in defining the focus areas and responsibilities for a new NIM for the Homeland.

In addition, the role of the Domestic DNI Representatives in improving the effectiveness of homeland intelligence remains ill-defined and needs to be clarified, as does their relationship to non-Title 50 partners and to a new NIM for the Homeland.

These two steps would reinforce the progress toward intelligence integration undertaken by the current DNI. Landmark undertakings to strengthen interoperability amongst IC components – such as the Intelligence Community Information Technology Environment (IC ITE) – are only beginning to take hold. Over time, the benefits to national intelligence should prove substantial and lasting, with the Enterprise a major benefactor.

Even after these steps are taken, much work remains to fully integrate homeland intelligence into the framework for national intelligence. A substantial segment of interviewees expressed a desire to see homeland intelligence collection and analysis requirements better coordinated. A preponderance of that segment identified the ODNI as the most logical focal point for setting priorities and requirements relevant to homeland intelligence, which would seem to be an appropriate responsibility for a Homeland NIM. ODNI’s newly instituted Homeland Threat Framework provides a basis for identifying and prioritizing threats, as well as relevant collection requirements and analytic priorities for IC agencies. The ODNI should present the requirements that cascade from the identified priorities in the Threat Framework as an addendum to the National Intelligence Priorities Framework (NIPF), which is designed to support the foreign intelligence mission. The Threat Framework could similarly be used to support the work of the Domestic DNI Representatives in prioritizing and aligning the work of IC elements across the United States, and in guiding their engagement with non-Title 50 partners both in and out of government. This framework could also inform the development of a dedicated Program of Analysis to guide members of the Enterprise and the IC in their efforts to focus and deconflict analysis on priority homeland intelligence issues.

INSA recommends that in addition to a separate NIM, the DNI designate a National Intelligence Officer (NIO) who could orchestrate homeland-related analysis requirements and responsibilities and work with the elements of the Enterprise (on a voluntary basis for those non-Title 50 organizations) to develop a Program of Analysis for the Homeland. Building on the identified priorities of the Framework, this work could also inform the development of a National Intelligence Estimate (NIE) to address key security threats that impact the homeland. An NIE, which would represent the consensus of the Intelligence Community, would be a landmark effort to document and analyze—in one place—the Homeland threat picture. The NIE’s analysis could be used to inform both policies to improve homeland security and future budget priorities for intelligence and non-intelligence agencies.

*“NIMs develop and oversee collection and analysis strategies for designated issue areas. As the DNI web site explains, “Appointed by the DNI, NIMs serve as the principal substantive advisors on all or specified aspects of intelligence related to designated countries, regions, topics, or functional areas. NIMs provide a single voice to policymakers to orient and guide collection and analytic activities to satisfy customers’ information needs. See Office of the Director of National Intelligence, “Intelligence Integration – Who We Are,” web site. Available at https://www.dni.gov/index.php/about/organization/intelligence-integration-who-we-are.”*
INTERAGENCY EXEMPLARS

Overall, interviewees from across the Enterprise expressed a sense of progress in interagency collaboration and cooperation. Stakeholders are recognizing the power of pooling information, authorities, and resources against a problem. Many viewed the National Counterterrorism Center (NCTC) as a model for federal-level interagency coordination and information sharing. Additionally, the FBI-led Joint Terrorism Task Forces (JTTFs), which are present in 104 cities, were praised for meaningful integration of federal and SLTT partners into FBI counterterrorism investigations. The Criminal Intelligence Coordinating Council (CICC) was cited by several interviewees as an organization that could play a bigger part in working with NCTC and other federal partners to enhance information sharing. Fusion Centers operated by state and local entities were recognized as critical nodes within a complex, national network that also includes other decentralized organizations like the JTTFs and High Intensity Drug Trafficking Areas (HIDTA) Program. Since INSA’s last report in 2011, interviewees were more unified in their support of Fusion Centers, focusing more on how to take them to the next level rather than debating whether they should exist at all.

FUSION CENTERS: TAKING THEM TO THE NEXT LEVEL

Each Fusion Center—formed and maintained by law enforcement or public safety agencies in states or major urban areas—serves as the primary focal point within a jurisdiction for the receipt, gathering, analysis, and sharing of threat-related information among public safety and security partners, including law enforcement, fire services, emergency responders, public health officials, critical infrastructure owners, and the private sector. Fusion Centers have helped authorities in states and major urban areas to fulfill specific roles and share information in an effort to address gaps identified in the wake of the 9/11 attacks. Federal partners must invest in building deeper relationships with Fusion Centers and continue to provide support in the form of deployed personnel, training programs and dedicated grant funding.
As Fusion Centers continue to mature and fill the state and local niche within the Enterprise, they have developed robust inter-organizational networks vertically, with federal partners and front-line safety and security personnel, as well as horizontally across jurisdictions nationwide. Numerous examples have emerged illustrating the value of a decentralized network that can rapidly disseminate information to and from front-line law enforcement and other public safety professionals in jurisdictions – large and small – across the nation. While many of these success stories are affiliated with non-terrorism related criminal activities ranging from human and drug trafficking to apprehension of murder suspects, the network can be leveraged on a daily basis by intelligence organizations across all levels of government seeking to disrupt terrorism-related activities or to determine such activities’ connections to their jurisdictions.5

Despite considerable progress across the national network, the maturity and effectiveness of Fusion Centers varies considerably, and some Fusion Centers struggle to fully integrate state and federal players and to penetrate organizational and cultural barriers between agencies. The need for integration extends beyond simply connecting databases and sharing digital information; partners across all levels of government still need to fully embrace the “need to share” mentality that encompasses digital and human networks.

In order for Fusion Centers to move to what some described as “Fusion Center 2.0,” Fusion Centers need relationships and communication with other Fusion Centers to ensure horizontal sharing, as well as a strong federal presence to facilitate vertical sharing. Currently, the FBI has little permanent presence in Fusion Centers, DHS has multiple personnel working in states and urban areas who are not assigned to the local Fusion Center, and private sector participation is minimal, varying widely from location to location.

It is also important to improve the connection between Fusion Centers and local private industry, in particular with the owners and operators of critical infrastructure. Indeed, given the nationwide presence of Fusion Centers with access to federal, state, and local threat information, they are ideally suited to serve as the focal point for federal engagement with private sector infrastructure operators.

One of the challenges Fusion Centers continue to face is the difficulty of establishing an analytic capability. Fusion Centers, many of which are small to begin with, experience high personnel turnover at the analyst and senior leadership levels, hampering analytic progress and diminishing institutional knowledge. At its most basic, this is a resource challenge. As federal grant funding diminishes, jurisdictions are actively seeking to retain their Fusion Centers through other funding vehicles that require an “all hazards” focus on local public safety issues other than terrorism. Such a change in focus requires staff with training, skills, and experience related to such local issues, which further distances fusion centers from the national Homeland Enterprise.

Part of the value proposition of Fusion Centers is the ability to produce intelligence products that add value within their jurisdictions while also contributing to federal partners and others in the Enterprise. In order to do this, federal partners must invest in building deeper relationships with Fusion Centers and continue to provide support in the form of deployed personnel, training programs, and dedicated grant funding. By continuing federal investment in the national network, federal agencies can help build stable partnerships at the state and local level among traditional and non-traditional safety and security partners, and enhance their ability to leverage the network by tapping into localized expertise and resources spread across the Nation.

Organizations with a stake in homeland issues would need to develop relationships and repeatable processes to facilitate the use of joint task forces when appropriate.

**FORMING TASK FORCES**

Several interviewees shared examples of working relationships and best practices that could promote collaboration – particularly by enabling organizations governed by disparate legal authorities to deepen mission understanding, strengthen operational support, improve collection and analysis, and enhance responsiveness to customer and stakeholder requirements. Agencies should expand and routinize the creation of task forces that assemble personnel from diverse stakeholder organizations to focus on a common problem. Such ad hoc task forces can draw, as needed, on intelligence and law enforcement agencies at the federal, state and local levels, as well as on private sector officials, to ensure that the organization has the information and authorities to address the challenge at hand. Task forces can be established on a permanent basis, as has been done by NCTC and the Joint Interagency Task Force-South (JIATF-S), or on a temporary basis to deal with a specific and time-limited problem, such as an interagency task force established to address the surge in unaccompanied minors crossing the U.S. border illegally in 2014. (See sidebar.)

While such interagency mechanisms offer interoperability across numerous statutory and organizational boundaries, interviewees cautioned that they cannot be created for every issue. Such an approach is costly, inefficient, and inflexible and must be based on a careful assessment of the purpose, mission, and most effective mix of Title 50, non-Title 50, and non-Federal participants. Second, the organizations with a stake in homeland issues would need to develop relationships and repeatable processes to facilitate the use of joint task forces when appropriate.

**TASK FORCES: A MODEL FOR NON-TRADITIONAL INTELLIGENCE ISSUES**

The immigration crisis that occurred in 2014, which included a surge in unaccompanied children from Central America seeking entry to the United States, is a potential model for future homeland-related crises. In response to the surge of unaccompanied immigrant minors, a whole-of-government effort was commissioned to address the influx and analyze and address its causes. The Intelligence Community was called upon to support the effort through the collection and analysis of relevant intelligence to help identify the root causes of the migration and the means by which individuals were moved to the U.S. border—often by means of smuggling organizations. To address this “non-traditional” intelligence issue, ODNI—working through the NIM and the NIO for the Western Hemisphere—established an interagency task force that brought together multiple agencies within and outside of the IC. This task force included representatives from Customs and Border Protection (CBP), Immigration and Customs Enforcement (ICE), the Federal Emergency Management Agency (FEMA), and the Departments of State and Health and Human Services (HHS), which collaborated to develop requirements, leverage diverse information sources, and develop a greater understanding of the issue. The work of the task force informed response measures, public awareness campaigns that warned of the dangers of the travel, and policy efforts to address the root causes of the immigration surge. The Task Force demonstrated the power of the interagency to come together in new ways and unite non-traditional partners to address difficult challenges.
COLLOCATION AND EMBEDDING OF PERSONNEL

Interviewees frequently raised the benefits of collocating organizations in the same facility and/or embedding liaison officers in joint organizations. One federal officer in the Enterprise praised the success of embedding his officers in joint organizations, which he credited for improving communication and understanding of organizational cultures. He believes that the most effective approach would be to collocate analysts, investigators, and interdiction personnel on common problems—in essence, creating task forces.

The Joint Counterterrorism Analysis Team (JCAT) is an excellent example of embedding personnel in a joint organization. It places cleared state and local law enforcement officers, first responders, and public safety professionals alongside federal counterterrorism analysts at NCTC. These individuals are charged with educating the national CT community on their SLTT requirements, helping to craft useful and actionable products, and mining IC information for information of use to SLTT and figuring out how to share it. They are essentially customer advocates for the entire SLTT community.

While many interviewees viewed collocation as a preferred solution in some instances, specifically JTTFs and Fusion Centers, the fiscal and bureaucratic obstacles to moving established brick-and-mortar organizations make embedding liaison personnel a more attractive and achievable option. Fusion Centers require support in strengthening participation by the key federal stakeholders, FBI and DHS, and placing emphasis on developing lateral relationships with their logical partners, JTTFs, and HIDTAs. Perhaps most importantly, embedding personnel in joint organizations fosters a shared sense of purpose and mutual understanding between partners that is not possible through the sharing of data and systems alone. Several interviewees emphasized the importance of embedding personnel to achieve a truly integrated approach to homeland security problems. Leveraging the strengths and distinct authorities of disparate offices can more effectively answer policymaker and operator questions.

INFORMATION SHARING

Thanks to the maturation of cross-functional bodies like Fusion Centers, JTTFs, and JCAT, information sharing across the Enterprise has become a more comfortable exercise in the years since the INSA 2011 white paper. Credit must also go to the office of the Program Manager of the Information Sharing Environment (PM-ISE), which has led the community in establishing standards and processes for information systems to house data and make the data accessible to authorized users from federal, SLTT, and private sector partners. Initially established by IRTPA to facilitate sharing of counterterrorism information, PM-ISE’s mission since has been broadened in recognition of the wider scope of homeland security requirements.

The decision to house the PM-ISE within the ODNI’s Partner Engagement office is a sensible step, but more remains to be done to leverage the networks and standards created by PM-ISE in support of national and homeland intelligence. PM-ISE should work with other elements of the ODNI and the IC to develop a repeatable process for sharing national information needs with SLTT and private sector partners and receiving information from those partners.
IMPROVING SHARING TO SLTT ENTITIES

Interviewees affiliated with SLTT entities or those who work closely with them identified a need to make information from federal partners more actionable and more timely. In the latter case, delays continue to be created by the challenges of declassifying information or downgrading the classification through unclassified “tear-line” reports that can be widely shared. Some interviewees also expressed frustration with the proliferation of competing information systems used by federal partners to share information with SLTT entities. The PM-ISE’s responsibility to create a whole-of-government Information Sharing Environment was overlaid on top of the FBI’s longstanding relationships with law enforcement and on DHS responsibilities to share information with law enforcement and private sector partners, particularly those managing critical infrastructure. Some progress has been made in collapsing multiple systems, but dissatisfaction remains among SLTT partners. Due to the multiple Departments and missions involved, streamlining to a single system may be impractical, but PM-ISE should examine where more consolidation is possible so as to reduce the burden on SLTT of multiple, non-compatible systems for accessing federally provided information.

IMPROVING SHARING FROM SLTT ENTITIES

The interviews revealed a great appreciation for the useful information and expertise that SLTT law enforcement can provide to address a range of national and homeland priorities beyond counterterrorism. To better leverage this information, SLTT entities would benefit from (1) a channel through which to understand the information needs of federal partners, (2) a well-defined mechanism for sharing information with the Intelligence Community, and (3) a training vehicle to educate personnel on information-sharing guidelines.

Regarding the first point, no uniform process exists for federal agencies to share national priorities and information requirements with SLTT entities. Second, even if SLTT entities do know what the national requirements are, they have no well-defined, easy mechanism for reporting that information in a way that can be ingested and used by the IC. Third, both federal and SLTT agencies report confusion about what is appropriate and legal for them to share. The IC cannot “task” SLTT entities, which operate under different legal authorities and restrictions. Federal and SLTT agencies (as well as their private sector partners) must develop guidelines for sharing information requirements and data in ways that are appropriate, legal, and respectful of civil rights and civil liberties. DHS/I&A has an infrastructure devoted to delivering training to SLTT partners that could be leveraged for this purpose (and which, in fact, already provides some of this type of training); however, no curriculum or training vehicle for federal components of the Homeland Enterprise exists.
IMPROVING SHARING WITH THE PRIVATE SECTOR

The majority of those interviewed stressed that private sector engagement in protecting critical infrastructure from both physical and cyber threats is of increasing importance and yet still has a long way to go to be properly defined and integrated into the overall homeland intelligence effort. On the government side, the Intelligence Community has an important role to play in identifying, analyzing, and communicating threats regarding U.S. critical infrastructure. DHS has primary responsibility within the federal government for managing federal efforts to protect this critical infrastructure, working closely with FBI, other federal Departments, SLTT partners, and private sector infrastructure operators. Given that the private sector owns and operates 85 percent of U.S. critical infrastructure, the Intelligence Community, the Homeland Enterprise and the private sector must ensure a robust flow of information and shared insights among all key partners.

We applaud ODNI’s recent efforts to develop a comprehensive assessment of national security threats to U.S. critical infrastructure and identify the means to capture key relevant intelligence requirements to better enable the IC to identify emerging threats. This work will better position DHS and other sector-specific agencies identified in the Presidential Policy Directive for Critical Infrastructure Security and Resilience (PPD-21) to support the needs of critical infrastructure. DHS I&A is the best-positioned agency in the IC to carry on this work for the long term, integrating its efforts with the National Programs and Protection Directorate (NPPD).

Going forward, it will be essential to ensure a robust interchange of information and insights between the federal government—to include the IC—and private operators of critical infrastructure. The focus to date has largely been on the flow of information from the government to the private sector, but the reverse is also essential. As such, DHS/I&A should form a working group to promote interactive feedback between private sector partners, the IC, and other federal partners in areas related to counterterrorism, public safety and other identified homeland security priorities. To support such an effort, DHS should establish a collaborative critical infrastructure team comprised of cleared representatives from the 16 critical infrastructure sectors. Such a body could be modeled after the Joint Counterterrorism Assessment Team (JCAT) within the National Counterterrorism Center, where cleared state and local first responders and public safety professionals work alongside federal counterterrorism analysts to inform their work and help ensure that state, local, tribal, and territorial entities receive the information they need at the lowest possible classification level. Establishing a similar entity for critical infrastructure protection would help ensure that private sector expertise and perspective inform the work of DHS and other federal organizations, and that they shape intelligence products to best meet the needs of critical infrastructure owners and operators.

CONCLUSION

No discussion of homeland intelligence activities and responsibilities would be sufficient without acknowledging the prevailing responsibility to protect civil liberties and respect citizens’ right to privacy. Many of the 2011 recommendations partially or directly advised how homeland intelligence may be conducted by federal, SLTT, and private sector partners within privacy and civil liberties safeguards. Since then, unauthorized disclosures have heightened public scrutiny of intelligence activities in support of homeland security and national security objectives. The subsequent public discourse in part has been hindered by a failure to distinguish between national, foreign, and homeland intelligence, underscoring the importance of arriving at publicly digestible and accepted definitions. To bolster public trust, the IC has taken steps to improve transparency and promote civil liberties. This includes the ODNI’s issuance of Principles of Intelligence Transparency for the Intelligence Community in October 2015 and establishment of the Intelligence Transparency Council in April 2016. The Council’s charter will expire no earlier than 2021, ensuring the work to promote transparency, engender public trust, and uphold civil liberties and privacy protections will continue for the near future.

While not explicitly covered in these recommendations, privacy and civil liberties protections in activities across the Homeland Enterprise demands considerable attention. As noted in 2011, the public should be an active participant in protecting the homeland; the DHS “See Something, Say Something” campaign is the most prolific of these engagement initiatives. Without public trust, Homeland Enterprise is not only diminished in operational effectiveness but also symbolically: citizens should not feel they need to be protected from the government. As the Enterprise and its many stakeholders seek to strengthen coordination of requirements, interagency cooperation at the federal level and information sharing with SLTT partners, privacy and civil liberties should be the foundation upon which enhancing cooperation and sharing is built.
SUMMARY OF RECOMMENDATIONS

INSA recommends the following for stronger integration and unity of effort across homeland intelligence activities:

1. **The next Administration** should clarify the DNI's role in coordinating and integrating all aspects of national intelligence and review the IRTPA and other intelligence statutes, regulations, EO's and related policies to ensure their consistency and adequacy for this purpose.

2. **The Office of the Director of National Intelligence** should integrate the Homeland Threat Framework into the National Intelligence Priorities Framework as a means to identify key national security threats to the homeland and align intelligence collection requirements and analytic priorities accordingly.

3. **The Director of National Intelligence**, in close coordination with the DHS Under Secretary for Intelligence and Analysis and the FBI National Security Branch Executive Assistant Director, should designate a NIM for the Homeland and an NIO for the Homeland, and seek to include key non-Title 50 representatives on the NIM Staff. The new NIO should create a Program of Analysis for homeland intelligence and commission an NIE based on the threats contained in the Homeland Threat Framework.

4. **The Office of the DNI** should clarify the roles of and guidance to the Domestic DNI Representatives, to include the appropriate mechanisms and procedures for interacting with non-Title 50 partners.

5. **The Program Manager of the Information Sharing Environment (PM-ISE)** should work with other elements of the ODNI and the IC to develop a repeatable process for sharing national information needs with SLTT and private sector partners and receiving information from those partners. PM-ISE should also work to reduce the burden on SLTT of multiple, non-compatible systems for accessing federally provided information.

**JOINT RECOMMENDATIONS FOR ODNI, DHS, AND FBI**

1. Expand and routinize the use of joint task forces organized around a common issue or problem set, comprised of personnel from intelligence, law enforcement, other operational organizations, and the private sector, as appropriate.

2. Encourage agencies to embed personnel into joint organizations to facilitate information-sharing and to foster a shared sense of purpose and mutual understanding that is not possible through the sharing of data and systems alone.

3. Enhance and maintain federal and private sector representation in Fusion Centers, and emphasize Fusion Centers as the focal point for federal engagement with SLTT partners.

4. DHS I&A should establish a working group to facilitate interactive feedback with the private sector related to critical infrastructure, counterterrorism, public safety, and other identified priorities.

5. DHS/I&A should develop training for federal, SLTT and private sector participants in the Enterprise regarding the appropriate and lawful collection and sharing of information, building upon existing training in privacy, civil rights and civil liberties.

6. DHS should establish an entity focused on critical infrastructure that draws on private sector expertise and shapes intelligence products to meet the needs of critical infrastructure owners and operators.
APPENDIX A

RECOMMENDATIONS FROM SEPTEMBER 2011 INSA WHITE PAPER

INTELLIGENCE TO PROTECT THE HOMELAND:
TAKING STOCK TEN YEARS LATER AND LOOKING AHEAD

1. Define Homeland Security Intelligence as “information that upon examination is determined to have value in assisting federal, state, local, and tribal and private sector decision makers in identifying or mitigating threats residing principally within US borders.”

2. The President, Congress and the Director of National Intelligence (DNI) should embrace a Homeland Security Intelligence Enterprise (Enterprise) characterized by fully connected federal, state, local and tribal law enforcement and public safety agencies, as well as private partners as required, with broadly defined and overlapping counterterrorism responsibilities focused on the coordination of intelligence and analysis efforts, not hierarchical command and control.

3. To ensure unity of effort within the Enterprise, the President and Congress should reaffirm the critical role of the DNI in providing strategic direction, coordinating homeland security intelligence activities, setting standards, and establishing priorities to drive collection and the development of required capabilities. It is important that the DNI, in partnership with the Secretary of Homeland Security and Attorney General, ensure that the elements of the Enterprise understand their responsibilities and stress accountability for their actions.

4. The DNI, in consultation with appropriate departments and federal agencies and state, local and tribal law enforcement leaders, should clearly identify a coordination body to facilitate, deconflict and encourage the adoption and implementation of necessary standards to drive connectedness for and in the Enterprise.

5. The DNI, in coordination with the Secretary of Homeland Security and the Director of the FBI, and in consultation with state, local and tribal leaders, should develop and implement foundational analytical training standards across the Homeland Security Intelligence Enterprise to ensure mission partners have common skills and understanding to communicate and collaborate. This will effectively facilitate integration of the diverse communities and establish trust and respect within the Enterprise. The DNI should consider developing a comprehensive homeland security training and education program to be offered to all elements of the Enterprise through the National Intelligence University. This should include comprehensive training on the imperative of respecting privacy, civil rights, and civil liberties.
6. The DNI, in partnership with the Office of Intelligence and Analysis, DHS, the Director of the FBI and state, local and tribal leaders should articulate a clear, lawful role for fusion centers in the national intelligence process and the national intelligence strategy, and define what constitutes appropriate Federal presence in a fusion center. DHS, I&A as the federal executive agent, should establish standards for training all fusion center analysts to a common analytic standard.

7. The DNI, in consultation with the Director, FBI, the Secretary, DHS, and state, local and tribal leaders should encourage interaction between FIGs, JTTFs, and fusion centers with regard to production and sharing of HSI, including the development of common operating procedures.

8. Congress should consider funding a base-line operational capability for state and urban area fusion centers. Federal funds should be limited to support of maintaining federally-validated capabilities, and allocated specifically for the fusion centers.

9. DHS I&A, in close coordination with the FBI and in consultation with state, local, and tribal leadership, should develop a common, robust, nationwide system for requesting information and receiving a timely response to ensure unity of effort in the Enterprise.

10. The Program Manager - Information Sharing Environment should develop policy for a single, effective suspicious activity reporting system, a better methodology and analytics to support the use of SAR reporting in HSI analysis, and promulgate policy for the establishment of a single sensitive but unclassified information sharing network for the Enterprise.

11. The U.S. Government and its state, local, tribal and private partners should develop a strategy and firmly commit themselves to a fully resourced, institutionalized, meaningful, and sustainable Community Engagement Program and encourage its implementation at the local level.

12. The U.S. Government and its state, local, tribal and private partners should continue to seek opportunities to include the public into the Enterprise through such programs as the DHS “See Something, Say Something” campaign.

13. The Program Manager-Information Sharing Environment should promote a decentralized environment in which disparate analytic nodes can communicate with each other and share knowledge. Technology should be the enabler but should not replace the analyst. New technology is not necessarily required but rather more effective integration and optimization can be made of existing systems and those under development.

14. The DNI should develop and recommend policies that foster greater connectedness and eliminate barriers to legal information sharing and collaboration among the tens of thousands of federal, state, local, tribal, and private sector entities that comprise the Enterprise.

15. The Chief Information Officer, ODNI should lead a follow-on effort to better identify what would be required to fix the patchwork of data management standards across the Enterprise, and how to leverage the power of technology to support and enforce privacy and civil liberties.

16. The DNI should ensure that privacy and civil liberties protections are fully integrated into statutes, policies, and procedures governing the Enterprise, requesting legislative support, as required.
INSA HOMELAND SECURITY INTELLIGENCE COUNCIL

HSIC brings current and former officials from DHS, FBI and other national and state law enforcement agencies together to articulate the critical importance of intelligence capabilities and operations to protect U.S. citizens. One of HSIC’s primary areas of emphasis is the need for more effective information sharing between federal agencies and its State, Local, Tribal, and Territorial (SLTT) partners.

ABOUT INSA

INSA is the premier intelligence and national security organization that brings together the public, private and academic sectors to collaborate on the most challenging policy issues and solutions. As a nonprofit, nonpartisan, public-private organization, INSA’s ultimate goal is to promote and recognize the highest standards within the national security and intelligence communities. INSA has over 160 corporate members and several hundred individual members who are leaders and senior executives throughout government, the private sector and academia.