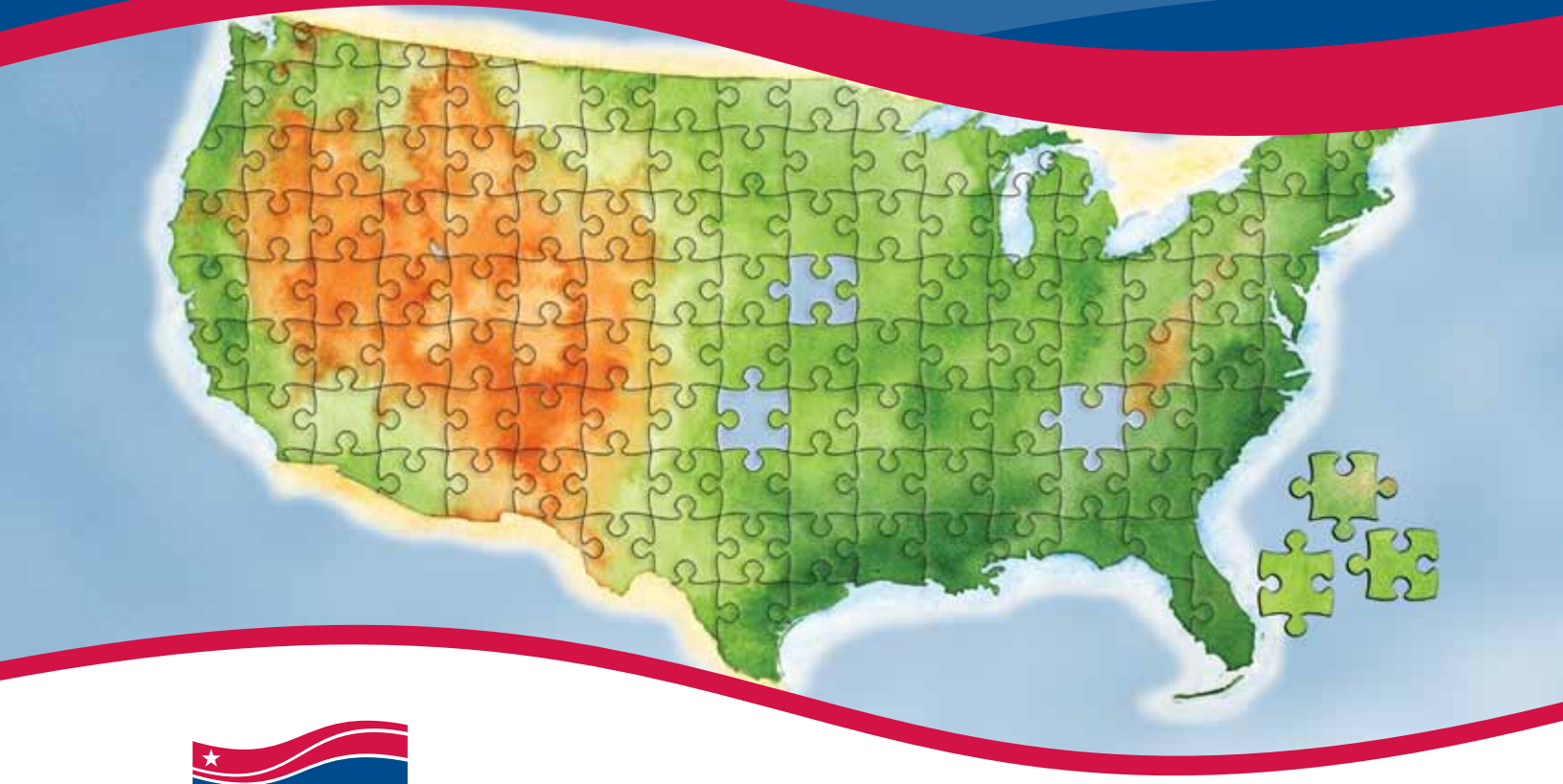
INTELLIGENCE TO PROTECT THE HOMELAND

...taking stock ten years later and looking ahead...



INSA

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

HOMELAND SECURITY INTELLIGENCE COUNCIL

SEPTEMBER 2011

ACKNOWLEDGEMENTS

INSA CHAIRWOMAN

Frances Fragos Townsend

INSA SENIOR INTELLIGENCE ADVISOR

Charlie Allen

INSA STAFF

Ellen McCarthy, *INSA President*

Chuck Alsup, *INSA Vice President for Policy*

Amanda Misko, *INSA Senior Research Intern*

Jeff Lavine, *INSA Director of Management and Marketing*

PARTICIPANTS IN THE HOMELAND SECURITY INTELLIGENCE COUNCIL

Chair and Co Chairs**

Joe Rozek, *Chair, Microsoft Corporation and the Center for Strategic and International Studies*

Kathleen Kiernan, *Co-Vice Chair, CEO Kiernan Group Holdings*

Laura Manning Johnson, *Co-Vice Chair*

Special Advisors**

Tom Finan, *Homeland Security Professional*

Philip Mudd, *Oxford Analytica*

Tom Ridge, *Ridge Global*

Suzanne Spaulding, *Bingham Consulting Group*

Governance Board**♦

Maureen Baginski, *Serco*

William "Bill" Gaches, *Northrop Grumman Corporation*

Stephen Kaplan, *Booz Allen Hamilton*

John Lauder, *Areté Associates*

Jennifer Sims, *Georgetown University*

Council Members by Subcommittee**

Definition

*Robert Riegle, *Mission Concepts Inc.*

*Marie O'Neill Sciarrone, *BAE Systems*

Bradford Gregg, *Booz Allen Hamilton*

Joe Nimmich, *Pennsylvania State University*

Development and Integration of the Homeland Security Intelligence Enterprise and Public Engagement

*Michael Rolince, *Booz Allen Hamilton*

Michael A. Brown, *U.S. Government*

Chris Leeman, *U.S. Government*

Don Loren, RADM USN (ret.), *Tauri Group*

Karen Morr, *SAIC*

Megan Woolsey

Full Integration of the Enterprise: the Ecosystem

*Michelle Farr, *LMI*

Tip Clifton, *Eastport Analytics, Inc.*

Suzanne Devlin, *BAE Systems*

Peter L. Higgins, *1SecureAudit*

Rosemary Lark, *KeyPoint Government Solutions*

John A. Russack, *Northrop Grumman Corporation*

Joseph Trindal, *KeyPoint Government Solutions*

The Privacy and Civil Liberties Mission

*Dan Prieto, *IBM and the Center for Strategic and International Studies*

Mary Ellen Callahan, *Homeland Security Professional*

Brooke Dickson-Knowles, *Scitor Corporation*

Alex Joel, *Office of the Director of National Intelligence*

**Denotes role of Chairman of a subcommittee*

***Participation on the Council does not imply personal or official endorsement of the views in the paper by any participating member or his/her respective parent organization(s).*

♦ *The Governance Board served exclusively in an advisory capacity*

INSA SUPPORTS A HEALTHY PLANET

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

INTRODUCTION

In the aftermath of the tragic events of 9/11, Americans slowly came to the realization that while the country had spent considerable national treasure on intelligence capabilities over the years to protect the nation and had prevailed in the Cold War for which the U.S. Intelligence Community (IC) had largely been designed, this IC was not designed, equipped, or ever primarily intended to detect significant national security threats originating or residing within our nation's own borders. Instead, it had been a long-standing and unique set of circumstances that had allowed Americans the good fortune of feeling safe within those borders. This sense of security was facilitated by two oceans and the Gulf of Mexico; two friendly neighbors to the north and south along relatively peaceful land borders; and a long history wherein immigrants, who are the lifeblood of this nation, came for opportunity and a hopeful future for their children, not to try to destroy the nation.

> Homeland Security Intelligence is a discipline that depends on the successful fusion of foreign and domestic intelligence to produce the kind of actionable intelligence necessary to protect the homeland.

In that environment, there was no perceived need for a robust national intelligence gathering capability within the U.S. for any purpose other than catching Soviet-era spies and serious drug traffickers. While other criminal activities presented challenges, they were handled relatively well by a complex, well-trained and decentralized law-enforcement system operating under strict Constitutional and other legal norms. Prior to 9/11 some observers expressed concerns about threats at home due to globalization, the changing dynamics of immigration, and the rise in extremism and radicalization associated with ethnic strife, poverty, and lack of opportunity in many parts of the post-Cold War world. Still, no one advocated for a significant domestic intelligence capability to address them. That all changed on September 11, 2001.

Following the 9/11 attacks, the need for a better domestic intelligence capability to keep Americans safe without violating their privacy, civil rights, and civil liberties was obvious, but how to achieve it was not. A Terrorist Threat Integration Center was formed that has since, through law, become the National Counterterrorism Center (NCTC). In March 2003, the Department of Homeland Security (DHS) was formally established. Moreover, following the release of the 9/11 Commission Report in July 2004 and the subsequent passage of the Intelligence Reform and Terrorism Prevention Act of 2004, a new cabinet-level post—a Director of National Intelligence—was created in April 2005 with the responsibility to oversee and coordinate all U.S. intelligence activities, foreign and domestic. Shortly thereafter in September 2005, the FBI formed its National Security Branch to focus on lawful intelligence gathering in the U.S. Each of these entities is critically important in its own right. However, integrating their respective efforts and efficiently and legally sharing information with law enforcement officials and other first responders at the federal, state, local, and tribal levels has proven to be a challenging task.

Throughout the ensuing policy debates regarding the proper role of domestic intelligence, the idea of establishing a separate intelligence agency similar to MI5 in Great Britain has been regularly discussed by pundits and politicians alike. Perhaps unsurprisingly, few of these discussions progressed very far—instead devolving into emotional arguments regarding the establishment of an intelligence agency to "spy" on U.S. citizens, legal residents and others physically within the country. To advance the dialogue, Congress directed DHS to commission an independent study by the Rand Corporation on the feasibility of creating a domestic intelligence agency. That study, published in 2008, did not make specific recommendations, but looked at pros and cons of various options, including a separate agency associated with the Department of Justice; a new agency within the existing FBI; and various policy and resource changes to improve the existing construct. That no action was taken as a result of this study speaks volumes to the difficulty and complexity of this issue.

The fact that there has not been another major terrorist attack on the U.S in the decade since 9/11 has given rise to the argument that the IC and its law enforcement and public safety partners are doing better at detecting and preventing such attacks and have received the legal and policy support that has enabled them to effectively work together. However, there have been several "near-misses" at home and abroad—including the Christmas Day Bomber in Detroit; the Times Square bomber; and the 2006 transatlantic aircraft plot—that have exposed persistent shortcomings in the nation's efforts. Additionally, the troubling trend of violent "homegrown" extremists, at home and abroad, personified by such persons as Timothy McVeigh and Major Nidal Hasan, continues to expose the IC's and law enforcement's difficulties regarding the detection of such internal threats.

Underpinning our analysis is the foundational principle that respect for privacy and civil liberties is an inherent, inseparable part of our national security and core values as a nation.

This paper takes the position that, currently, there is no interest or political will to establish a new and separate agency to take on the very necessary, but still controversial domestic intelligence responsibilities. The challenge, therefore, is to assess what current capabilities exist at the national level, as well as at the state and local levels, to do this work and to determine which capabilities might be improved to optimize the nation's security posture. Given the looming fiscal imperative to reduce federal, state and local spending, the successful completion of this task has taken on even greater importance.

This paper likewise posits that domestic intelligence is not a panacea for protecting the homeland. In most cases, particularly terrorist plots motivated by extremist ideologies, threats to the homeland have both domestic and foreign components. For that reason, this paper will address the concept of homeland security intelligence (HSI) – a discipline that depends on the successful fusion of both components to produce the kind of actionable intelligence necessary to protect the homeland.

This paper will propose a fundamental working definition for HSI, review some of the key challenges to the effective execution of the HSI mission, and discuss ways to better connect the various practitioners of HSI into a more collaborative, integrated enterprise. Underpinning this analysis is the foundational principle that respect for privacy and civil liberties is an inherent, inseparable part of our national security and core values as a nation.

THE CHALLENGE

Homeland security professionals dislike the "connect the dots" analogy for analyzing data to catch terrorists. It seems to trivialize a very difficult, complex, but essential task. Caryn Wagner, Under Secretary for Intelligence and Analysis (I&A) at DHS, described the challenge best by likening the management of all the disparate data that might prove useful to counterterrorism to finding most of the pieces of a dozen massive jigsaw puzzles mixed in a pile—with no pictures to help make sense of your goal—and then sorting through all the pieces to figure out each puzzle.[1]

Caryn Wagner described the challenge best by likening the management of all the disparate data that might prove useful to counterterrorism to finding most of the pieces of a dozen massive jigsaw puzzles mixed in a pile—with no pictures to help make sense of your goal—and then sorting through all the pieces to figure out each puzzle.

The Intelligence and National Security Alliance (INSA) Homeland Security Intelligence Council (the Council) has labored over the past year to assess the current state of our ability to develop intelligence to protect the homeland and formulate suggestions that could improve the ability of the IC and its unique network of partners to protect the nation. We specifically looked at what would be required to create an effective Homeland Security Intelligence (HSI) framework and how an enabling enterprise could be organized to maximize the utility of that framework in fighting terrorism in the United States.[2] Except in general terms, we do not address the specific architecture or membership of the Homeland Security Intelligence Enterprise (the Enterprise). That should be the subject of a separate study and paper. Ten years after the 9/11 attacks, we believe it is time both to acknowledge our advances in developing HSI and to renew our efforts in improving and using it. Based on this year-long review by approximately 40 homeland security professionals[3], we believe that we should do the following to improve HSI:

1. Adopt a common definition of Homeland Security Intelligence to facilitate its collection, analysis, use in decision making, and development as a discipline;

2. More fully connect the federal, state, local and tribal law enforcement and intelligence agencies with broadly-defined and overlapping counterterrorism responsibilities and, as appropriate, partners from the private sector, into an Enterprise characterized by coordination of intelligence and analysis efforts, not command and control;

3. Seek opportunities to include the public into the Enterprise, such as by encouraging citizens to respond to the DHS "See Something, Say Something" campaign to provide information that may result in suspicious activity reporting (SAR)[4] and community engagement with isolated immigrant communities and other potentially disconnected and disaffected elements; and,

4. Ensure the protection of privacy and civil liberties as a core intelligence mission through widely applicable training and accountability standards in order to promote the lawful yet aggressive detection and deterrence of terrorist operatives in the homeland.

This paper presents recommendations for how to accomplish these suggestions and summarizes them at its end. Each recommendation is more fully developed and explained in three related papers on key challenges, the unique skillsets and tradecraft needed to operate in this unique HSI ecosystem, and civil liberties imperatives associated with the conduct of HSI as identified through the Council's year-long analysis and review of this specialized area. We recommend that readers seeking additional information read each of these papers, posted on the INSA website at www.insaonline.org.

DEFINING HOMELAND SECURITY INTELLIGENCE

Arguably, one of the reasons HSI has not developed faster as a discipline is because it lacks a functional definition. Accordingly, the Council has developed a working definition and strongly recommends its adoption:

> *"Homeland Security Intelligence is information that upon examination is determined to have value in assisting federal, state, local, tribal and private sector decision makers in identifying or mitigating threats residing principally within U.S. borders."*

Terrorism threats are complex and adaptive; thus, our response must be equally adaptive while being agile, resilient, highly collaborative and highly connected in order to enter and disrupt the terrorists' decision cycle.

This definition encompasses all-source analysis of traditional intelligence and law enforcement information; public reports under the DHS "See Something, Say Something" campaign; and all other legally collected information, both foreign and domestic, that is useful in identifying or mitigating threats.[5] Mixing data from these disparate sources to create actionable counterterrorism (CT) intelligence was unthinkable before 9/11. Today, the need for hybrid HSI—with appropriate privacy and civil liberties protections in place—is at the heart of the recently released National Strategy for Counterterrorism that envisions a non-traditional, whole-of-nation approach to protecting the public against terrorism. The strategy states:

> *"U.S. CT efforts require a multidepartmental and multinational effort that goes beyond traditional intelligence, military, and law enforcement functions. We are engaged in a broad, sustained, and integrated campaign that harnesses every tool of American power—military, civilian, and the power of our values—together with the concerted efforts of allies, partners, and multilateral institutions."*[6]

> One of the tools the strategy highlights is "information sharing among law enforcement organizations at all levels." The strategy goes on to say,

> *"…in the Homeland, the capabilities and resources of state, local, and tribal entities serve as a powerful force multiplier for the federal government's CT efforts. Integrating and harmonizing the efforts of federal, state, local and tribal entities remains a challenge. As the threat continues to evolve, our efforts to protect against those threats must evolve as well."*

Information sharing alone is not enough to make a whole-of-nation effort against the terrorist threat we face. Terrorism expert Bruce Hoffman, of Georgetown University, has stated that few terrorist organizations during the 20th Century lasted more than a year and still fewer more than five years—relatively short "lifespans" that typically did not allow for thorough understandings of the organizations or the threats they posed. According to Hoffman, the terrorist organizations that have lasted are marked by the keen ability to adapt to changing conditions in pursuit of their strategies: to wear down enemies through economic attrition, prolonged military deployments, strengthening local and regional affiliates and lone wolf attacks. Hoffman argues that operations in the United States are the ultimate goal of these longer lasting terrorist organizations.[7] Major General (MG) Michael Flynn, a former senior intelligence officer in Iraq and Afghanistan and a recognized expert on counterterrorism and counterinsurgency, reinforced Hoffman's views by observing that the terrorist enemies America faces not only adapt, but also exhibit the continuing ability to learn quickly and apply lessons from previous operations, regardless of success.[8] Accordingly, the nation's defensive measures must be faster, more flexible, and more applicable to constantly changing situations posed by our adversaries. A non-traditional organizational structure will likely be required in order to succeed in the implementation of such agile defensive measures.

Rarely is information gathered from traditional criminal investigations valued, shared or fused with other information into a better understanding of the operative's intent.

The federal government, moreover, cannot fulfill this mission alone. Most terror operatives in the last decade have been undetected through traditional intelligence or federal law enforcement sources alone. The broad, sustained, and integrated campaign of terrorism waged against the United States—domestic terrorism most especially—gives off a weak intelligence signal and consequently requires closer observation to identify. For example, terrorist operatives have traveled to the United States and sometimes have lived otherwise normal lives in plain sight as they planned their attacks against the homeland. In other cases, operatives have used the United States as an operational planning site for attacks outside the country. Furthermore, as media reports have increasingly demonstrated, even several American citizens have become radicalized to the point of violence. As citizens, however, they are highly unlikely to be in intelligence reports. Such operatives give few clues as to their intentions that could be picked up from traditional human intelligence, electronic collection, or other IC tradecraft. The few clues that do exist are more like Under Secretary Wagner's pile of mixed puzzle pieces—making little sense without some broader context or direction. Terrorism threats are complex and adaptive; thus, our response must be equally adaptive while being agile, resilient, highly collaborative and highly connected in order to enter and disrupt the terrorists' decision cycle.

State, local, and tribal law enforcement officers are critical new partners to HSI who can provide precisely that insight. These officers have routinely interacted with terror operatives during their investigations of traditional criminal activities. In hindsight, we often discover that these traditional crimes—drug sales, money laundering, forgery, cigarette tax evasion, and others—were used to support terrorist operations. Rarely, however, is this information valued, shared, or fused with other information into a better understanding of the operative's intent. Maureen Baginski, former FBI Executive Assistant Director for Intelligence, and Shawn Henry, current FBI Executive Assistant Director of the Criminal, Cyber, Response, and Services Branch, both agree that many federal intelligence and law enforcement officers do not recognize the homeland security implications and intricacies of criminal information.[9] MG Flynn attributes this disconnect to either a lack of information sharing or a lack of recognition of the value of information, even if shared. He believes it should be incumbent on the federal government to share lessons learned in the greater war on terror with state, local, and tribal law enforcement officers, and to train them on the evolving tactics, techniques, and procedures that have been developed in response. The observations and recommendations contained in this paper are designed to help homeland security professionals improve their ability to connect and collaborate to detect and recognize legitimate threats, develop analytic capabilities to make the information easier to process, and strengthen the roles of key counterterrorism partners.

HOMELAND SECURITY INTELLIGENCE ENTERPRISE

Jennifer Sims, Director of Intelligence Studies at Georgetown University believes that "decision advantage is the desired end state" that homeland security intelligence should provide. Decision advantage requires analysts to provide actionable intelligence to those decision makers who have the authority to take decisive action against the terrorism threat. Development of policies, techniques, and procedures, as well as the infrastructure to support a connected Homeland Security Intelligence Enterprise enabling collaboration and cooperation among these whole-of-government counterterrorism analysts will be essential for mission success. Together they will support a decision advantage for federal, state, local and tribal leaders and law enforcement officers, and will better position the nation to prevent terrorist attacks.

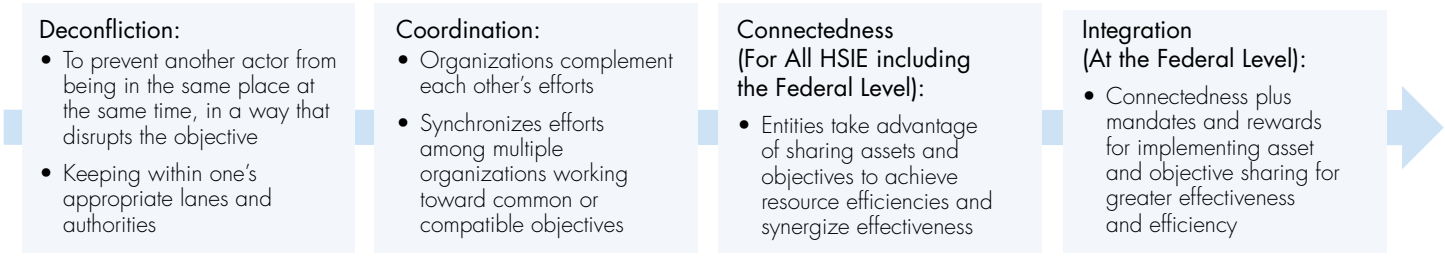


Figure 1: Spectrum of Connectedness[11]

To be most effective, a HSI framework must facilitate the connection between the elements of the Enterprise, to include local law enforcement and other first responders. The envisioned Enterprise would be characterized by coordinated collaboration, not command and control. In effect, this would create a loose confederation of all IC, law enforcement, and public safety analysts nationwide working collectively to achieve the success of the broader mission they share—preventing terrorism in the United States. This will improve unity of effort especially in already recognized areas of overlap within their complex missions: all source analysis and production of counterterrorism intelligence products in support of operations. This overlap of authorities is a fundamental part of our fabric as a nation and part of our unique heritage. If embraced and leveraged the right way, it is not a problem, but rather a strength to be maximized. In other words, a multitude of different entities with different perspectives and different operational patterns overlapping in the same mission space will provide multiple opportunities to detect and react to threats. For this concept to work, the Enterprise must function not as a hierarchy but as a confederation of equal partners who agree to unifying principles. It would be helpful for the DNI to suggest these principles and implementation standards. This Enterprise would, however, require a coordination body to provide a venue for deconfliction and establish training and collaboration standards that will drive connectedness. To ensure success, the DNI would need to designate such a coordinating body, in close coordination with the FBI and DHS I&A, and after extensive consultation with state, local and tribal leadership.

CONNECTEDNESS

FUSION CENTERS AND PARTNERS

For the Enterprise to be most effective, it must fully understand and be responsive to decision makers' information requirements. When it comes to protecting the nation from a terrorist attack, the relevant intelligence collectors, analysts, and the final decision makers will be in different agencies and departments at different levels of government or within the private sector in some cases (e.g., when the threat vector is a cyber attack on the nation's critical infrastructure). At the same time, intelligence generated for one operational entity may have relevance to more than one Enterprise member—in many cases in a way that was not originally understood by the original analyst. Unity of effort among the disparate members of the Enterprise accordingly requires development of a networked approach, such as the one established among the 72 state and major urban area fusion centers working with FBI Field Intelligence Groups (FIGs) and Joint Terrorism Task Forces (JTTFs) and connected to DHS I&A and NCTC. Such a networked structure will facilitate a linkage that promotes an effective, disciplined, common system for requesting information and receiving a response. To optimize this unity of effort, all elements of the Enterprise including nontraditional partners of the IC, such as other federal agencies, (e.g., Transportation Security Administration, Immigration and Customs Enforcement, and Customs and Border Protection), as well as, state, local, and tribal law enforcement partners, should share common analytical training standards.

> The national security enterprise must reach beyond the capabilities of the federal government and the IC to identify and warn about impending plots that could impact the homeland, particularly when the individuals responsible for the threats operate within the United States and do not travel or communicate with others overseas.

Over the last decade, the federal government, every state, and several major urban areas have partnered to establish a National Network of Fusion Centers designed to be the primary focal point within the state and local government for the receipt, analysis, gathering, and sharing of Homeland Security Intelligence between the federal government and state, local, and tribal partners. These fusion centers were initially created for counterterrorism information sharing and analysis purposes, but many today encompass all-crimes and all-hazards approaches. They are uniquely situated to empower front-line law enforcement personnel and public safety analysts to understand local implications of national intelligence and facilitate the lawful gathering and sharing of information to identify emerging threats, thus enabling local officials to better protect their communities. In close cooperation with FIGs and JTTFs, fusion centers represent a foundation upon which to build a strong Homeland Security Intelligence Enterprise.

I&A serves as the executive agent for leading federal government-wide support for fusion centers and has helped coordinate the provision of federal funding, technical assistance, security clearances, and access to classified networks. Additionally, DHS

has assigned intelligence liaison officers to most fusion centers with the mission to support their analytical efforts, facilitate information sharing between the federal government and state, local, and tribal partners, and provide training. There has been important progress since fusion centers were established by state and local, governments in the years following September 11, 2001, but capability building to a common standard among all centers remains a challenge due to diminishing budgets at the state and local level and a shortage of trained intelligence analysts.

To increase its relevancy, the National Network of Fusion Centers must be able to provide actionable intelligence in support of operations and contribute to strategic warning and Enterprise planning. This will take the centers far beyond their information sharing paradigm and will require the Enterprise to develop a better system for requesting information and being assured of a timely response. Phillip Mudd, former Deputy Director, Counterterrorism Center, Central Intelligence Agency and former Deputy Director, National Security Branch, Federal Bureau of Investigation, stated that such a system should be customer-oriented, providing a two-way street of information sharing between federal law enforcement on the one hand and state, local, and tribal authorities on the other.[12] To effectively accomplish this goal, it is essential that fusion centers focus their efforts on existing all-crimes and criminal intelligence activities to leverage existing information, skills, knowledge, and expertise, while avoiding duplication of efforts at the federal, state and local level.

In the case of terrorism, fusion centers serve as points of integration for state and local officials into federal law enforcement operations through the JTTFs and FIGs associated with FBI Field Offices. This partnership will ensure a coordinated counterterrorism approach among all levels of government. The Enterprise must reach beyond the capabilities of the federal government and the IC to identify and warn about impending plots that could impact the homeland, particularly when the individuals responsible for the threats operate within the United States and do not travel or communicate with others overseas. Fusion centers are well-positioned to gather and share such information from state and local partners across the Enterprise, particularly with JTTFs and FIGs. This type of information is necessary to pursue and disrupt activities that may be indicators of, or potential precursors to, terrorist activity. Likewise the FIGs are equally well-positioned to share transnational terrorist threat information with fusion centers. This example of connectedness facilitates a whole-of-government approach to protecting the public against terrorism.

Intelligence generated for one operational entity may have relevance to more than one Enterprise member—in many cases in a way that was not originally understood by the creator of the original analysis.

As federal, state, local, and tribal governments confront a challenging fiscal environment, there will be increasingly difficult questions regarding the effectiveness of the fusion centers, FIGs, and JTTFs. The President's National Security Strategy (May 2010) states: *"To prevent acts of terrorism on American soil, we must enlist all of our intelligence, law enforcement, and homeland security capabilities. We will continue to integrate and leverage state and major urban area fusion centers that have the capability to share classified information; establish a nationwide framework for reporting suspicious activity; and implement an integrated approach to our counterterrorism information systems to ensure that analysts, agents, and officers who protect us have access to all relevant intelligence throughout the government."*[13] Developing of measures of effectiveness will be critical in assessing the importance of these capabilities in protecting our nation.

THE ECOSYSTEM

IMPROVED CONNECTEDNESS OF THE ENTERPRISE

While the National Network of Fusion Centers, in partnership with FIGs and JTTFs, appears to be the logical foundation for the Enterprise, the reality is that the Enterprise is much more complex and amorphous. Ultimately, all intelligence, law enforcement, and public safety analysts with valuable information should be able to connect within this Enterprise, person-to-person across disciplines, with appropriate protocols regarding privacy, civil rights, and civil liberties. This would be the final stage of the culture shift in information sharing that started following 9/11. David Bray, author of *Knowledge Ecosystems: A Theoretical Lens for Organizations Confronting Hyperturbulent Environments*, stated, "no one individual harbors sufficient knowledge to either mitigate negative outcomes or capitalize on positive opportunities" and therefore, analysts must "transcend physical group proximity and the institutions themselves" to gather the information needed.[14] MG Flynn found this to be true in Afghanistan and called for this kind of networked analysis in his paper, "*Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan*," particularly from the analysts in closest contact with the population. This networked, bottom-up approach requires intelligence professionals who not only have deep substantive expertise and solid analytical skills, but also have the ability to reach out to and collaborate with analysts who can add information or insights, as needed.[15]

Ultimately, all intelligence, law enforcement, and public safety analysts with valuable information should be able to connect within the Enterprise, person-to-person across disciplines with appropriate protocols regarding privacy, civil rights, and civil liberties.

HSI will have fully developed as a distinct intelligence discipline when it functions seamlessly as an analyst-to-analyst system across organizational boundaries. At that point, it will reach its highest value in protecting the homeland from significant threats, particularly terrorism. The system will require unique, and not yet identified, analytic frameworks, knowledge management, collaboration tools, and training that include built-in safeguards for privacy, civil rights, and civil liberties protections for U.S. persons. Over time, the system would optimally build new information sharing platforms and technical solutions. Until that time, it will rely on smart analysts communicating and sharing to the best of their ability in a manner that meets applicable legal, regulatory, and policy guidance.

ENGAGING THE PUBLIC

The National Strategy for Counterterrorism envisions an integrated campaign that harnesses every tool of American power. The American public is an invaluable part of that effort.

Public contributions to SARs through the DHS "See Something, Say Something" campaign provides particularly valuable, but hard-to-analyze, information for HSI. As a terrorist operation approaches the moment of execution, preparations, such as surveillance and moving weapons into place, provide observable and abnormal activities that citizens recognize and frequently report. Some of these observations make it into validated SAR reports. According to former Los Angeles Police Officer, Commander Joan T. McNamara, many law enforcement officers believe that SARs are not intelligence products in and of themselves; instead they are a significant part of the threat data that, when properly analyzed, forms the basis of useful HSI.[16] DHS/I&A Principal Deputy Under Secretary Bart R. Johnson commented, "as proven by recent events, our state, local, and tribal partners are most familiar with the citizens, institutions, and critical infrastructure in their communities—they are best positioned to see and report suspicious activities."[17] Clearly, SAR data has significant value to homeland security analysis, although developing the right analytic tools and methods to maximize SAR potential remains a key challenge.

Public contributions to Suspicious Activity Reports through the DHS "See Something, Say Something" campaign provides particularly valuable but hard to analyze information for HSI.

Additionally, there is an important whole-of-nation role for a specific segment of the public—law-abiding, but sometimes disconnected and disaffected immigrant communities. Prior to 9/11, most law enforcement and intelligence agencies had little knowledge of, or meaningful interaction with, the Arab and Muslim-American communities. Such lack of connection is not a new phenomenon in the history of our multi-cultural, immigrant nation—it just happens to be the one we are experiencing now. Community engagement serves to reassure immigrant communities that they are a respected part of the population and that their active participation as part of the solution is essential to ensure the security and prosperity of our diverse nation. Meaningful engagement is also a significant source of information about violent radicalization and the role of foreign operatives in fomenting it. Like the DHS "See Something, Say Something" campaign, engagement can also help identify threats against isolated immigrant communities emanating from right-wing radical groups. Such concepts require a federally supported, formalized Community Engagement Program managed and implemented locally to help foster the long-term community partnerships that will build trust on all sides.

As noted above, recent events have focused attention on Arab and Muslim-American communities. This newly focused attention is likely a temporal phenomenon as the demographics of our nation continue to evolve. Community engagement must be viewed as a broad responsibility to embrace all components of our society and to be watchful of any trends that are causing any element of society to become radicalized This allows for early detection of trends that might identify bad actors who are taking advantage of or living in these immigrant communities for nefarious purposes.

CIVIL LIBERTIES: THE FOUNDATION OF SECURITY

The Council argues that whole-of-nation protection against terrorism can be achieved in tandem with the nation's values when it comes to privacy, civil rights, and civil liberties. The Constitution and existing laws and regulations allow for a significant range of action by intelligence and law enforcement officials that must be well-known and understood by those officials and the public alike. An underlying premise of this paper is that respect for the rights of individuals is the very foundation of our national security.

> Privacy, civil rights, and civil liberties protective measures must become a way of life for the HSI professional.

The tragic events of 9/11 challenged our understanding of national security risks. Asymmetric threats to homeland security—including economic security—are now understood to potentially emanate from both outside and within America's borders. Accordingly, the perception of what constitutes homeland security intelligence must expand to include state, local, and tribal law enforcement as new players with new information that traditionally had not been part of the national security paradigm. As such, the rise of the Homeland Security Intelligence Enterprise has been paralleled by an increasing focus on the essential role that privacy and civil liberties protections must play in this expanded environment.

Privacy and civil liberties responsibilities must be woven into the core business logic of the Enterprise in order for the Enterprise to be effective. All homeland security professionals are obliged to respect and protect privacy, civil rights, and civil liberties by the oath they take to protect and defend the Constitution. At the same time, there is extraordinarily high pressure to put the puzzle pieces together; a task complicated by the fact that those puzzle pieces have grown more and more complex given the increasingly diverse information that is being gathered, analyzed, and shared to promote situational awareness about threats to the homeland. This situation makes it imperative that privacy, civil rights, and civil liberties protective measures be designed and implemented as part and parcel of homeland security intelligence efforts. "Privacy by design" means that such protections are "built in" and not "bolted on" to the core efforts of organizations that participate in the Enterprise. It must become a core value of each member of the Enterprise. Privacy, civil rights, and civil liberties protective measures must not be viewed narrowly as a compliance or back-office function of concern only to legal or information technology officers. On the contrary, it must become a way of life for the HSI professional.

The Enterprise must embrace a dual mission for all intelligence analysts of ensuring security as well as preserving privacy, civil rights, and civil liberties. Since 9/11, the core mission of the Enterprise has been to prevent attacks. Citizens have legitimate concerns that overly aggressive efforts to predict and prevent attacks could lead to misuse of sensitive personal information. Managers of the Enterprise must prevent actual infringements and avoid any perception that intelligence analysts are pushing the envelope or testing the limits of the Constitution. In order to build this public confidence, intelligence analysts must be trained and rewarded for embracing both security and protecting privacy, civil rights, and civil liberties as two sides of the same coin. The rules must be understood, followed, supported, and promoted as part of the core mission of all intelligence practitioners. This ethic, and accountability to that ethic, will help convince the American people that this important intelligence effort to protect their homeland is worthy of their trust.

Intelligence analysts must be trained and rewarded for embracing both security and protecting privacy, civil rights, and civil liberties as two sides of the same coin.

There is no robust framework for harmonizing privacy rules and privacy-related information-management practices (including data retention) across organizational boundaries in the Homeland Security Intelligence Enterprise. A number of agencies in the Enterprise have issued privacy guidelines and implemented their own information management rules and regulations regarding such things as data security retention. Enterprise organizations each possess senior privacy and civil liberties officers. The law, moreover, requires that information sharing be consistent with privacy and civil liberties considerations. These existing authorities may be sufficient for an individual organization, but their sum total is a relative patchwork that does not comprise a sufficiently robust and coherent system to govern privacy and civil liberties across the entire homeland security intelligence spectrum.

As one example, timelines for the disposal of privacy-protected information vary widely among intelligence and law enforcement organizations. Federal intelligence agencies can retain U.S. persons data for 90 days for analytic purposes. However, law enforcement agencies can legally hold onto that same information for 30 years as part of an open criminal investigation. Inconsistencies, gaps, tensions, or conflicts will be exacerbated as data volumes and information sharing across organizational boundaries increase—a problem likely to be compounded by the growing threat of data loss or theft. Consistency and harmonization of these and other related regulations would more convincingly secure the public's trust regarding privacy, civil rights, and civil liberties.

The appointment of privacy, civil rights, and civil liberties officers within departments (at various levels of seniority) without an overarching framework or coordinated approach risks the inconsistent application of the law and its protections. Some attempts have been made to address this concern through the creation of interagency bodies and the White House Privacy and Civil Liberties Oversight Board. However, mechanisms and a framework to ensure better coordination and oversight of privacy and civil liberties are not yet mature or have not been fully leveraged.

CONCLUDING THOUGHTS

The Enterprise described in this paper is a very complex, decentralized system. Through a probable combination of improved capabilities, better cooperation, experience, and good fortune, the few terrorist incidents that have occurred since 9/11 have either been averted or quite limited in scope. While the various elements of the Enterprise are better connected than before, they nevertheless have split loyalties between the individual agencies or communities they support and the Enterprise itself. Not surprisingly, their responsibilities to their parent organization will usually take precedence. Regardless, relatively effective collection, analysis, sharing, and operational response to Homeland Security Intelligence is happening. Although responsibilities for Homeland Security Intelligence at the federal level are split between multiple agencies, synergy of effort appears to be healthy. Similarly, the relationships between FIGs, JTTFs, and state and major urban area fusion centers are, for the most part, proving to be complementary and constructive. The challenge is how to make it more effective and to minimize the reliance on luck for mission success. Realistically, we will probably not be able to deter or detect every threat to our homeland, but it is a worthy goal to secure the cooperation of every element of the Enterprise to work collectively to protect it.

Robust dialogue by all players in the Enterprise regarding its future development is critical. Shifting a significant portion of the responsibility for homeland security intelligence analysis into the communities that would experience the attack—not just depending on Washington, DC—would energize the power of a whole-of-government approach. The Enterprise, building on the National Network of Fusion Centers working in close cooperation with FIGs and JTTFs will connect, support, and synergize that powerful, distributed network of analysts. The public has its role to play in this Enterprise through reporting observed anomalies (DHS "See Something, Say Something" campaign) that may lead to suspicious activity reporting, and through community engagement. Finally, we fail if, in the name of security, we jeopardize the privacy, civil rights, and civil liberties that make us the nation we are. We must find creative ways to work within the existing paradigm to be both secure and free. INSA Chairwoman and former Homeland Security Advisor to the President, Fran Townsend, put it most powerfully when she recently said,

> *"The continuing threat to the homeland is obvious. Terrorists continue to seek weapons of mass destruction, cyber and conventional capabilities to do us harm. It falls to the intelligence community, law enforcement at all levels, and other non-traditional partners to produce the homeland security intelligence that will protect our nation and still preserve our liberties. We have made improvements at this complex task over the past ten years, but the fact remains that we need to get even better because failure is not an option."*[17]

KEY RECOMMENDATIONS

- 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."

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

DEFINITIONS

Active Defense

A mobile and flexible continuum of federal, state, local and tribal actions to detect, deter, and prevent attacks by the enemy faster than the enemy adapts. Unlike a static defense, the enemies' tactics are ineffective because the defense is less predictable.

Ecosystem

A system formed by the interaction of a community of organisms with its environment.

Field Intelligence Groups (FIGs)

Embedded intelligence entities in each of the FBI's 56 field offices designed to fully integrate the intelligence cycle into field operations and manage the Intelligence Program in coordination with the Directorate of Intelligence at FBI Headquarters.

Homeland Security Intelligence (HSI)

Information that upon examination is determined to have value in assisting federal, state, local, tribal and private sector decision makers in identifying or mitigating threats residing principally within U.S. borders.

Homeland Security Intelligence Enterprise (Enterprise)

All federal, state, local and tribal analysts that plan, collect, process, analyze and disseminate homeland security intelligence.

Suspicious Activity Report (SAR)

Official documentation of observed behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal, or other illicit intention.

Terrorism

Terrorism is defined in the Code of Federal Regulations as "the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives" (28 C.F.R. Section 0.85).

Domestic Terrorism

The unlawful use, or threatened use, of force or violence by a group or individual based and operating entirely within the United States or Puerto Rico, without foreign direction, committed against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof in furtherance of political or social objectives.

International Terrorism

Violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or any state, or that would be a criminal violation if committed within the jurisdiction of the United States or any state. These acts appear to be intended to intimidate or coerce a civilian population, influence the policy of a government by intimidation or coercion, or affect the conduct of a government by assassination or kidnapping.

Whole of Government

Government, political leaders, law enforcement officers, and others officials at the federal, state, local and tribal levels.

Whole of Nation

This paper uses this term to include those within the definition of whole of government as well as the public.

FOOTNOTES

[1]*An Evening with Charlie Allen and Caryn Wagner, Under Secretary for Intelligence and Analysis, DHS, INSA Speaker Series Dinner, The Westin Arlington Gateway, November 17, 2010.*

[2]*For the purposes of this paper, we are looking at a terrorism plot or act that is targeted at locations within the United States, its territories or possessions. We do not distinguish by whether attackers are of foreign or domestic origin.*

[3]*See list of Council participants and contributors.*

[4]*For the purposes of this effort, we have not included the private sector in the realm of the public, although we recognize the significant difference.To do justice to the complex and difficult task of incorporating the private sector into the Homeland Security Intelligence Enterprise beyond its information sharing relationship to the Department of Homeland Security Infrastructure Protection effort and the Federal Bureau of Investigation through InfraGard requires a dedicated discussion beyond the scope of this paper. Similarly we have not incorporated the valuable role played by non-law enforcement members of the first responder community—fire fighter, public health professionals, etc. This would also require specific review best undertaken in another paper.*

[5]*For the purposes of our efforts we are concerned with the threat of terrorism in the United States, although we realize that Homeland Security Intelligence could be used against other threats.*

[6]*National Strategy for Counterterrorism, The White House, June 2011.*

[7]*Bruce Hoffman Georgetown University, Director of the Center for Peace and Security Studies, Interview, Homeland Security Intelligence Council Meeting, INSA offices, Date May 26, 2011.*

[8]*Major General (MG) Michael Flynn, U.S. Army, Interview, Homeland Security Intelligence Council Meeting, INSA Offices, June 9, 2011.*

[9]*Homeland Security Intelligence Board Meeting, Teleconference, June 16, 2011.*

[10]*Jennifer Sims Director of Intelligence Studies at Georgetown University interview, Homeland Security Intelligence Council Meeting, INSA Offices, May 26, 2011.*

[11]*"Maturing the Homeland Security Intelligence Enterprise," published on the INSA website www.insaonline.org, September 7, 2011.*

[12]*Phillip Mudd Former Deputy Director, National Security Branch, Federal Bureau of Investigation and Former Deputy Director, Counterterrorist Center, Central Intelligence Agency; interview, Homeland Security Council Meeting, INSA offices Date July 16, 2011.*

[13]*National Strategy for Counterterrorism, The White House, June 2011.*

[14]*David A. Bray, "Knowledge Ecosystems: A Theoretical Lens for Organizations Confronting Hyperturbulent Environments," in Social Science Research Network, June 2007 (http://ssrn.com/abstract=984600).*

[15]*Major General Michael T. Flynn, Captain Matt Pottinger, and Paul D. Batchelor, "Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan," Voices from the Field, Center for a New American Security, January 2010.*

[16]*Joan T. McNamara, Former Los Angeles Police Officer, Homeland Security Council Meeting, INSA offices, April 14, 2011.*

[17]*Remarks by DHS/I&A Principal Deputy Under Secretary Bart R. Johnson at "Fusion Centers: Function and Future" sponsored by the CSIS Homeland Security and Counterterrorism Program, in conjunction with the Homeland Security Studies and Analysis Institute (HSI) and the Homeland Security Systems Engineering and Development Institute (HS SEDI), February 24, 2011.*

[18]*Fran Townsend, Chairwoman of the Intelligence and National Security Alliance Board of Directors, Homeland Security Intelligence Council Meeting, July 27, 2011.*

INTELLIGENCE AND
NATIONAL SECURITY
ALLIANCE

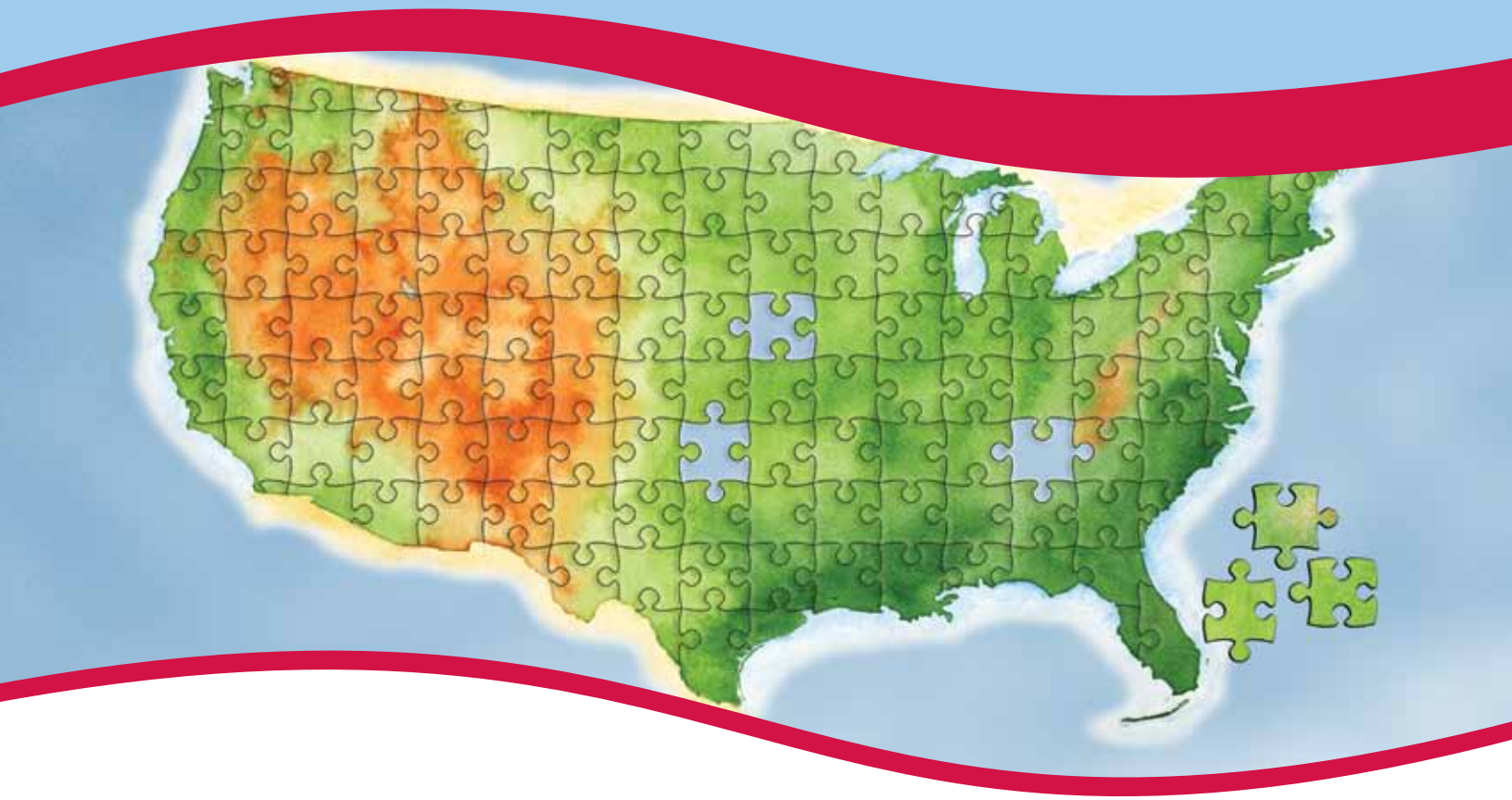
ABOUT INSA

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 non-profit, non-partisan, 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 150 corporate members and several hundred individual members who are leaders and senior executives throughout government, the private sector and academia.

To learn more about INSA visit www.insaonline.org.



INTELLIGENCE AND NATIONAL SECURITY ALLIANCE
SUPPORTING ADVANCES IN THE NATIONAL SECURITY AGENDA

901 North Stuart Street, Suite 205, Arlington, VA 22203
(703) 224-4672 | www.insaonline.org