OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Domestic Approach to National Intelligence

★ ★ ★ ★

UNITED TO PROTECT

Table of Contents

Preface

This publication comprises inputs from a broad array of participants representing elements of the U.S. Intelligence Community (IC) and its partners in the domestic field. We thank everyone involved for their time and valuable contributions.

The process began with meetings and resulted in many conversations, drafts, revisions, and rounds of coordination with subject matter experts, lawyers, privacy and civil liberties officials, and senior leadership. Over time, we realized the topic is very complex and often characterized differently by the various participants and stakeholders, depending upon their vantage point and mission. Segments explaining the role of specific IC agencies and departments were written and provided by the entity itself.

The Domestic Approach to National Intelligence describes the "as is," or current picture, of the operating environment for the IC's key engagements with federal, state, local, tribal, territorial, and private sector partners inside the United States. The next step—one that may be even more complex and challenging—is to move beyond the "as is" descriptions and work toward a vision of the "should be." Challenges aside, we owe it to the American people to strengthen the national security apparatus to best protect our citizens and their privacy, civil rights, and civil liberties.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

LEADING INTELLIGENCE INTEGRATION

Since my appointment as the Director of National Intelligence in 2010, one of my highest priorities has been strengthening intelligence partnerships to help preserve the country's national security. Partnerships have long been a foundation of our work overseas. In light of 9/11 and the rapidly evolving nature of foreign threats to the homeland, we also must renew our focus on how the Intelligence Community (IC) collaborates with partner agencies inside the United States to ensure that we carry out our national and homeland security missions as effectively as possible. Protecting the privacy and civil liberties of our citizens is fundamental to this endeavor.

Significant progress has been made since 9/11 in building capacity, standardizing practices, and sharing information with partners in the United States to defend against and respond to foreign and foreign-inspired threats to our homeland. As vital as that progress has been, I believe that we still have work to do to ensure that all those involved in this effort —including the American people—share a common understanding of how this mosaic fits together. Thus, I directed my staff to work with our partners to describe in a single document the "as-is" operating environment for the IC's key engagements with federal, state, local, tribal, territorial, and private sector partners inside the United States. The result of my request is the paper, *Domestic Approach to National Intelligence*.

This paper was prepared in consultation with the ODNI's Office of Civil Liberties, Privacy and Transparency and Office of General Counsel and coordinated with mission partners. Appropriately, the paper's description of the "as-is" operating environment reflects each agency's limitations imposed by law, policy, and mission, and highlights the importance of protecting privacy and civil liberties, an imperative for all partners engaged in this committed effort. The paper does not purport to describe the specific laws, policies, safeguards, or operations relating to each agency's activities, nor does it make recommendations for change.

I believe the *Domestic Approach to National Intelligence* provides, in a transparent manner, a common general understanding of the current state of intelligence exchange between the IC and its domestic mission partners, and serves to further our collaborative efforts. We trust that it will serve as a useful foundation for the ongoing, productive dialogue on homeland security that the American people rightfully expect.

James R. Clapper
Director

“ We need to deal with the realities of globalization – the blurring these days of foreign and domestic matters. Because when threats like terrorism and international organized crime transcend borders, it’s critical that we think holistically about intelligence. But we’re also a people who – Constitutionally and culturally – attach a high premium to our personal freedoms and our personal privacy.”

James R. Clapper

Purpose

This paper, the *Domestic Approach to National Intelligence*, describes certain key roles and relationships that characterize efforts by members of the U.S. Intelligence Community (IC) and federal, state, local, tribal and territorial (FSLTT) government organizations to engage with one another to carry out the shared mission of protecting the homeland. These partners work with one another, and through established channels with the private sector (e.g., critical infrastructure owners and operators), as part of a complex web of relationships. Each partner, regardless of level, plays an important role in protecting the homeland with respect to warning, interdiction, prevention, mitigation, and response. The importance of partnerships and collaboration is emphasized in this paper, as is the IC's responsibility to the public to protect privacy, civil rights, and civil liberties. Descriptions related to organizational responsibilities and/or authorities are provided by the respective agencies. The *Domestic Approach to National Intelligence* is consistent with the framework and recommendations outlined in the Criminal Intelligence Coordinating Council's (CICC) National Criminal Intelligence Sharing Plan, the strategies in support of the National Network of Fusion Centers, and information sharing and safeguarding standards outlined by the Program Manager for the Information Sharing Environment (PM-ISE).

By describing these roles and relationships in one place, this paper strives to foster an important national dialogue that will promote a better understanding of how the IC engages with key partners in this domestic enterprise and supports the holistic ideals articulated by the Director of National intelligence (DNI).

PROTECTING PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES

To prevent and deter acts of terrorism and other threats on American soil, we must continue to develop lines of coordination and appropriately align intelligence, law enforcement, and homeland security efforts. However, this must be accomplished only in accordance with the Constitution, laws, Executive Order 12333, and core values of our nation. Protecting fundamental rights and liberties is an important national security end in and of itself. The *Domestic Approach to National Intelligence* is fully committed to exemplifying America's values: operating under the rule of law, consistent with Americans' expectations for the protection of privacy and civil liberties, respectful of human rights, and preserving the trust of the American people. As President Obama stated at the National Archives in May 2009, "We uphold our fundamental principles and values not just because we choose to, but because we swear to. Not because they feel good, but because they help keep us safe. They keep us true to who we are… So as Americans, we reject the false choice between our security and our ideals. We can and we must and we will protect both." Thus, it is essential that we comply with all applicable legal and policy authorities including, but not limited to, the Privacy Act, Executive Order 12333, and the Information Sharing Privacy Guidelines. Similarly, IC elements and FSLTT organizations must continue to operate within their defined mission roles and responsibilities.

President Obama, photo provided by the White House

"We uphold our fundamental principles and values not just because we choose to, but because we swear to. Not because they feel good, but because they help keep us safe. They keep us true to who we are… So as Americans, we reject the false choice between our security and our ideals. We can and we must and we will protect both."

President Obama
National Archives in May 2009

(Opposite) Director Clapper briefing the President, photo provided by the White House

Challenge

Our nation must deal with a wide range of complex threats to our people and interests both overseas and within the nation's borders. These threats include foreign-based and foreign-inspired terrorism, foreign intelligence activities, homegrown violent extremism, transnational organized crime, cyber-attacks by foreign actors or their agents, and more. Shrinking budgets and growing mission requirements demand effective, interoperable, and non-duplicative–that is, "smart"–government operations. This new dynamic also demands greater teamwork and responsible information sharing between members of the IC and FSLTT partners—as well as appropriate and responsible information sharing with the private sector—that is consistent with law, policy, and regulation and protects privacy, civil rights, and civil liberties. Such partnerships provide access to the expertise and unique capabilities and authorities held by each partner, resulting in benefits not only to those involved but also to the nation as a whole.

As the nature of threats to the homeland changes, so too does the nature of the challenges the nation must address. Transnational organized crime poses a significant and growing threat to national and international security and bears dire implications for public safety, public health, the security of democratic institutions, and economic stability across the globe. For example, transnational drug traffickers and human smugglers operating across U.S. borders and within the U.S. reap enormous profits that enable them to undermine legitimate governance in their countries of origin. At the same time, international criminal organizations, terrorists, and state-sponsored cyber attackers have demonstrated their ability to compromise information systems. Many of these threats have low-level signatures. Detecting them and determining their attribution can be difficult.

Washington DC, photo provided by ODNI

9/11 Museum and One World Trade Center, photo provided by ODNI

The U.S. is considered a high-priority intelligence target by many foreign intelligence entities. While traditionally the threat has been to our political, military, and diplomatic interests at home and abroad, the loss of sensitive economic information and technology is a growing threat to our national security. In recent years, economic espionage conducted by foreign intelligence entities, corrupt insiders, and corporate competitors has exploited vulnerabilities in cyberspace that may weaken our economic advantage. Cyber espionage has not replaced traditional espionage as a way to steal secrets, but the ability to focus technology on lesser protected information is a significant and growing threat.

Even before the 9/11 attacks, the IC elements and FSLTT organizations started developing relationships to identify and address particular threats and national intelligence challenges in the homeland. There was, however, no integrated national approach. Since 9/11, significant progress has been made in building capacity, standardizing

CBP helicopter flying over New York City, photo provided by CBP

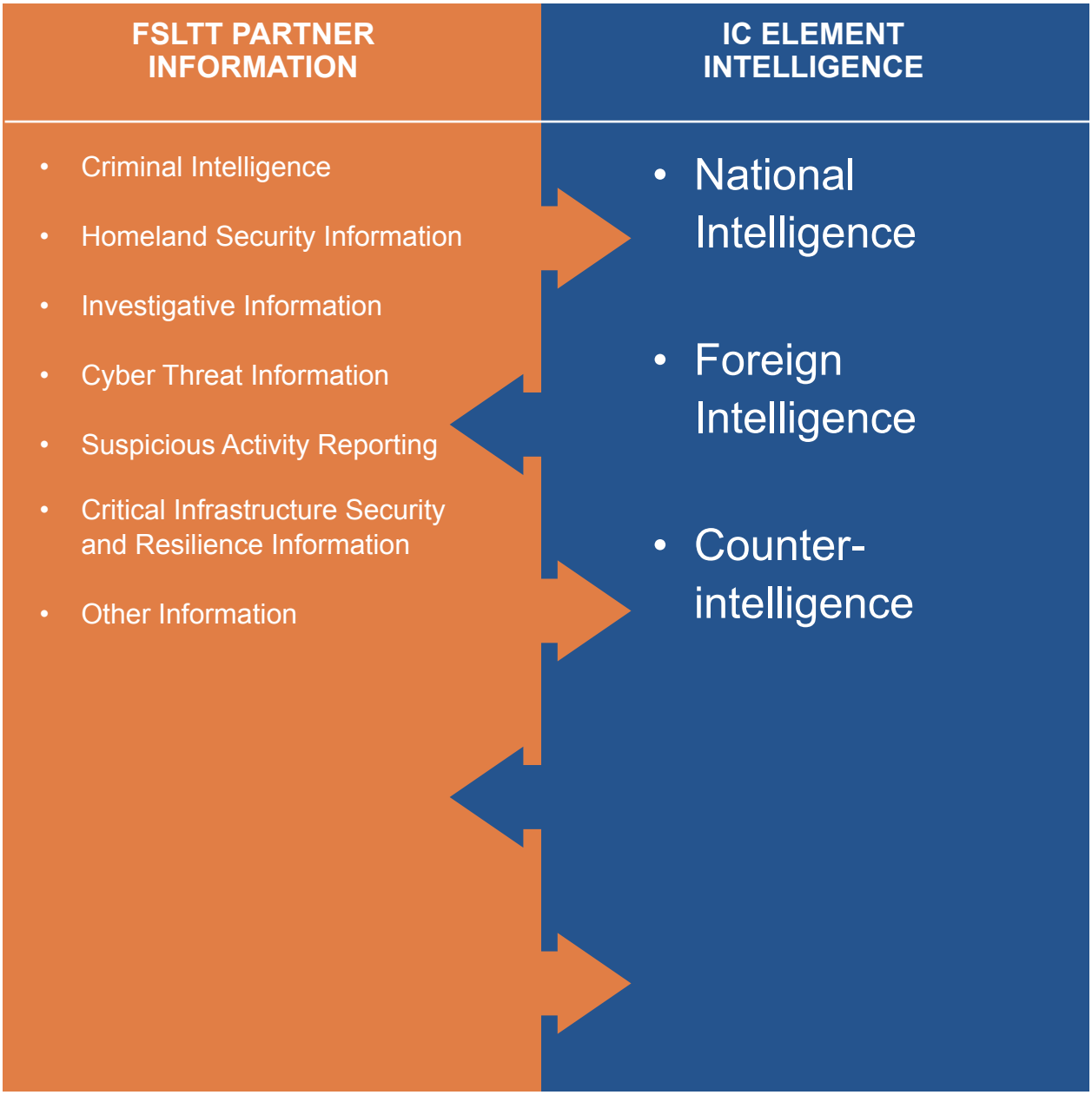
practices, and sharing information, both horizontally and vertically, to support foreign operations, perimeter protection, and homeland security and law enforcement (HS&LE) requirements. Nonetheless, inconsistent practices, absence of doctrine, and a lack of unity of effort across levels of government still characterize the domestic landscape. This domestic enterprise is more ad hoc and independent than organized and enterprise-oriented, and often depends more on personal or preexisting relationships than defined engagement protocols. Many potential stakeholders and contributors are left out of the equation as well, particularly on issues other than counterterrorism.

In navigating this enterprise, it is important for individual IC elements and FSLTT organizations to continue to work within their respective missions and authorities, even as they seek to enhance responsible collaboration and information sharing. In particular, the sharing activities and relationships between IC elements and FSLTT organizations are undertaken through established channels and in accordance with legal and policy requirements that are designed to ensure agencies are acting within their authorities and missions and are protecting privacy, civil rights and civil liberties. Sharing with the private sector is undertaken with special care so that applicable legal and policy requirements are identified and followed.

Integrating National Intelligence

The effective integration of national intelligence with relevant information from FSLTT partners is essential to protecting the nation. This integration requires agile, robust, and responsible processes that leverage existing partnerships and encourage new ones. These partnerships enable appropriate information sharing and build trust, consistent with the missions and authorities of each agency and the need to protect privacy, civil rights, and civil liberties. As trust and partnerships mature, efficient integration across stakeholders is also increased, resulting in an enhanced understanding of respective capabilities, information, and requirements (including how customers use products and services).

This graphic depicts some types of FSLTT information and intelligence shared in the domestic environment. In some cases, information can be categorized as both FSLTT information and intelligence.



ROLES & RESPONSIBILITIES

The IC interacts with and serves a wide range of customers and partners, both within and outside the U.S. Government (USG), with intelligence support designed to meet the customers' and partners' responsibilities and specific mission requirements.

Customers are those who have requirements for intelligence products or support, and use it to carry out their official responsibilities. Within the domestic enterprise, federal customers directly receive unique support from the IC based on their mission needs, often through a Federal Intelligence Coordination Office (FICO). With regard to state, local, tribal, and territorial (SLTT) customers, information categorized or derived from national intelligence is generally disseminated by the Department of Homeland Security Office of Intelligence & Analysis (DHS/I&A), the Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), and the U.S. Coast Guard (USCG). Dissemination occurs directly or via a "hub & spoke" approach through entities like fusion centers, and Joint Terrorism Task Forces (JTTFs). The wide-array of customers for intelligence support include departmental secretaries and senior policymakers, threat coordinators, governors, state homeland security advisors, mayors, police chiefs, sheriffs, first responders, federal officials, and others who are directly engaged in making decisions related to public safety. In addition, appropriate threat and warning information is provided to the private sector (e.g., owners and operators of critical infrastructures), through established channels.

New York City Police Department patrol cars, photo provided by NYPD

FSLTT partners include HS&LE organizations operating across our country to protect our borders, points-of-entry, infrastructure, and communities. These professionals are on the front line of ensuring public safety and protecting the nation from all threats. Partner preparedness is crucial to our national security, as they have the greatest visibility on local criminal activity relevant to national intelligence and will be the first responders on the scene during threat situations and incidents. Information sharing at this level supports law enforcement and public safety offices best equipped to understand current threats and the risks associated with them, inform resource allocation, and interdict or investigate criminal actors. Crucial to their efforts is the timely and efficient sharing of criminal intelligence, public safety, and open source information via communication networks designed to store and transmit Sensitive But Unclassified (SBU) information. These partners also play a critical role in identifying suspicious activities and reporting this information following protocols established by the Nationwide Suspicious Activity Reporting Initiative (NSI).

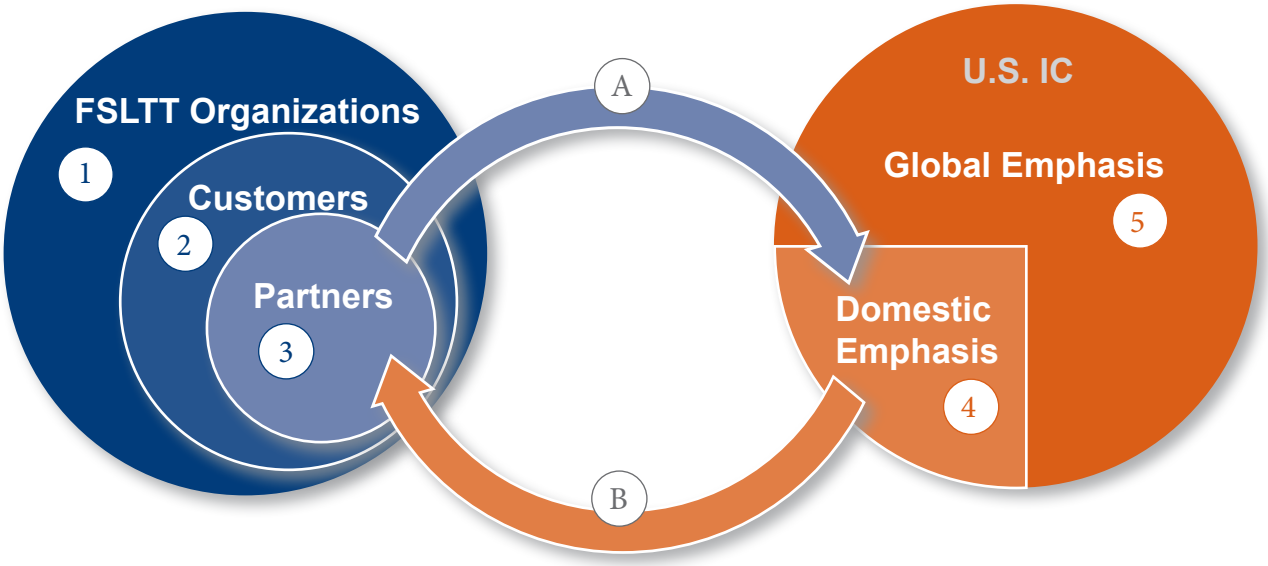
Immigration and Customs Enforcement Agents, photo provided by ODNI

Additionally, appropriate and responsible information sharing with private sector entities, particularly the owners and operators of infrastructure critical to national security whose businesses may be exploited by nefarious actors, is fundamental to the protection and resilience of the nation. Such sharing takes place through established channels and in accordance with applicable law and policies. Private sector organizations undertake security and threat mitigation measures to protect lives and property and have unique information and expertise that can help the IC and FSLTT better understand existing threats.

Thus, the domestic enterprise is characterized by an extraordinarily complex set of customer and partner relationships, composed of both informational and organizational architectures that are involved in the collection, analysis, use, and dissemination of information and intelligence. Relationships are described in general terms, recognizing that there is no national standard or doctrine for these interactions. It is also important to note that the descriptions on the following page do not include the multiple layers of legal and policy requirements that govern these relationships.

The Domestic Enterprise

This graphic broadly illustrates the relationships between FSLTT and U.S. IC partners.



1 **FSLTT Organizations**

Organizations operating on the front lines across the country to protect border points-of-entry, infrastructure, and communications, such as federal departments and agencies, DHS component agencies, local police departments, first responders, and other entities involved directly in infrastructure security and resilience.

2 **Customers**

Individuals that maintain a 'customer' relationship with the IC, such as governors, homeland security advisors, mayors, critical infrastructure owners and operators, and HS&LE leaders.

3 **Partners**

Organizations that carry out the intelligence cycle under their respective authorities and may maintain formal partnerships with the IC, such as fusion centers, High Intensity Drug Trafficking Areas (HIDTAs), Regional Information Sharing System (RISS) Centers, Criminal Intelligence Units (CIUs), and federal departments and agencies with FICOs.

4 **IC Elements with Domestic Emphasis**

Federal departments and agencies with both Title 50 and Non-Title 50 components, such as DEA, DHS, FBI (to include Field Intelligence Groups (FIGs), JTTFs, the Terrorist Screening Center (TSC)), and USCG. DHS/I&A and FBI are primarily responsible for the IC's domestic analysis and information sharing efforts with HS&LE partners.

5 **IC Elements with Global Emphasis**

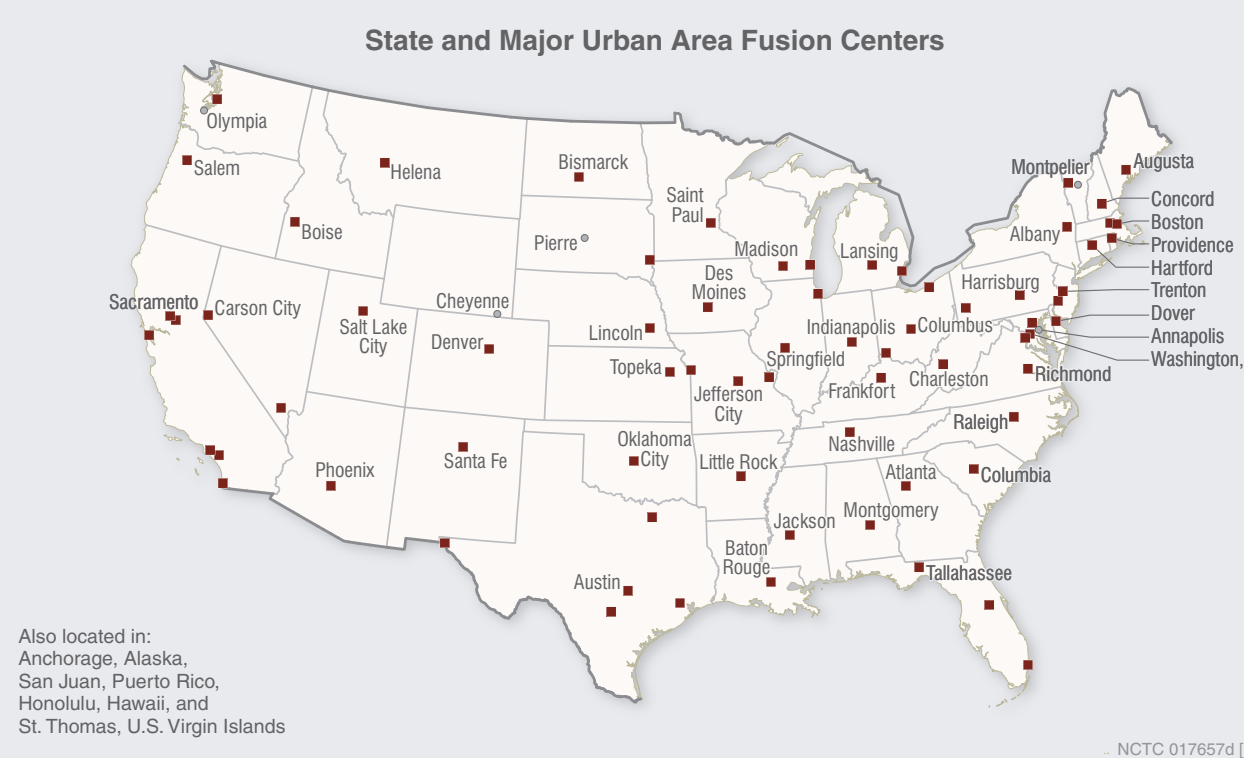
Federal departments and agencies that provide support to FSLTT partners, through appropriate channels, in the form of current intelligence, alerts, warnings, and notifications, such as CIA, DIA, NGA, NSA, etc.

A **SAR/NSI, Intelligence Information Reports (IIRs), Criminal Intelligence, and Investigative Information**

FSLTT-initiated processes for documenting, processing, analyzing, and sharing national intelligence with the IC.

B **Alerts, Warnings, Notifications, Bulletins, TTPs, and other intelligence reporting**

IC-initiated processes for documenting, processing, analyzing, and sharing national intelligence with FSLTT partners.



KEY FSLTT SHARING ORGANIZATIONS/FUNCTIONS

Certain FSLTT entities have formed specialized sharing organizations, or include specific sharing functions, that serve as points of intersection between FSLTT elements and the IC.

State and Major Urban Area Fusion Centers

The 78 federally-recognized fusion centers in the country form the National Network of Fusion Centers and operate to assist HS&LE partners in preventing and responding to crime, including terrorism. Fusion centers serve as focal points for the gathering, receipt, analysis, and sharing of threat-related information between partners. They are owned and operated by state and local entities with support from federal partners in the form of deployed personnel, training, technical assistance, exercise support, security clearances, connectivity to federal systems, technology, and grant funding. Located in states and major urban areas throughout the country, fusion centers are uniquely situated to empower front-line law enforcement, public safety, fire service, emergency response, public health, critical infrastructure owners and operators, and private sector security personnel with an understanding of the local implications of national intelligence. Additionally, fusion centers are optimally positioned to identify local, regional, and statewide trends regarding criminal or suspicious activity that relate to national security threats. Fusion centers provide interdisciplinary expertise and situational awareness to support decision making at all levels of government. Most fusion centers have access to SECRET-level systems, to include systems operated by DHS, FBI, and/or the Department of Defense (DOD). This connectivity enables fusion centers to obtain and review classified reports disseminated in accordance with applicable laws and policies.

High Intensity Drug Trafficking Areas (HIDTAs)

The Office of National Drug Control Policy (ONDCP) provides assistance via the HIDTA program to federal, state, local, and tribal law enforcement agencies operating in 28 areas determined to be the nation's critical drug trafficking regions. The program's goal is to reduce drug availability by assisting agencies participating in HIDTAs with federal support to dismantle and disrupt drug trafficking organizations, which includes analytic support to tactical counterdrug operations. Although many of the participating officers are cleared at the SECRET-level, the majority of their work is done at the UNCLASSIFIED and LAW ENFORCEMENT-SENSITIVE-levels. The HIDTA program is built on the premise that participating agencies should have an equal voice in addressing regional drug threats.

High Intensity Financial Crime Areas (HIFCAs)

The Department of the Treasury's HIFCA program is intended to concentrate law enforcement efforts at the federal, state, and local levels to combat money laundering in designated high-intensity money laundering zones. In order to implement this goal, a money-laundering action team was created or identified within each HIFCA to spearhead a coordinated anti-money laundering effort. Each action team is composed of all relevant federal, state, and local enforcement authorities, prosecutors, and financial regulators. Participating agencies leverage their respective authorities and resources to meet mission requirements. The seven HIFCA areas are California Northern District, California Southern District, Southwest Border, Chicago, New York, Puerto Rico, and South Florida.

Immigration and Customs Enforcement Agent, photo provided by ODNI

Regional Information Sharing System (RISS) Centers

The RISS network, funded by the DOJ's Bureau of Justice Assistance, consists of six centers across the country that provide tailored analytic, technical, and research support, database access, equipment loans, event deconfliction, and training to local law enforcement agencies. RISS centers operate at the UNCLASSIFIED and LAW ENFORCEMENT-SENSITIVE-levels.

Criminal Intelligence Units (CIUs)

CIUs serve as the principal collectors of criminal intelligence at the state and local law enforcement levels. Independently owned and operated by major city, major county, and state police law enforcement agencies, these intelligence units conduct strategic law enforcement intelligence operations on organized criminal activity, transnational threats, and terrorism within their jurisdictions. While separate and distinct from federal task forces and the IC, these units help support the analytic efforts of fusion centers and HIDTAs, contribute to federal task force investigations, and support other decision makers.

Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)

ATF strives to enhance public safety by protecting Americans from gun violence, the criminal misuse of explosives, and acts of arson. In support of these key missions, ATF also regulates the explosives and firearms industries. ATF's investigative and regulatory expertise is especially helpful due to its jurisdiction over firearms and explosives – two "commodities" that can possibly relate to terrorism and national security. At the headquarters-level, ATF maintains contact with several IC agencies through direct liaison positions within ATF's Office of Strategic Intelligence and Information. Additionally, ATF's intelligence analysts and supervisors maintain working relationships with such entities as the National Network of Fusion Centers, and JTTFs. Finally, ATF publishes Intelligence Information Reports (IIR) for the community at large, both at the classified and unclassified levels, and is in the process of posting formally published criminal intelligence reporting on various IC platforms.

Civil Applications Committee (CAC)

The CAC is an interagency committee led by the Department of the Interior that coordinates and oversees the federal civil use of classified and unclassified collections. Chartered by the President in 1975, the CAC provides federal civil agencies access to national systems data in support of their mission responsibilities. Specifically, it provides a forum through which the federal civil agencies coordinate data requirements, develop tasking strategies, certify the proper use of data, and track and plan for the progress and evolution of national systems. CAC activities have expanded beyond traditional mapping applications to a broad range of environmental and remote-sensing applications central to federal agency civil missions, such as monitoring recovery from natural disasters and related hazards. The CAC also coordinates the use of imagery exploitation and application resources and supports remote-sensing research and development activities at special facilities, such as the United States Geological Survey (USGS) Advanced Systems Center. Examples of CAC facilitated activity include monitoring volcanoes, detecting wildland fires, coordinating emergency response to natural disasters (such as hurricanes, earthquakes, and floods), monitoring ecosystems, and mapping wetlands.

Federal Intelligence Coordination Offices (FICOs)

Outside of the IC, numerous federal departments or agencies have staff charged with intelligence-like functions. Cleared to the TOP SECRET levels, many with access to classified networks, FICOs serve as an interface between the IC and federal partner communities. FICOs provide varying levels of support to senior policymakers and consumers of intelligence/information within their organization. Examples of departments with a FICO include the Federal Reserve Board of Governors, Department of Transportation, and Department of Commerce. Federal Senior Intelligence Coordinators (FSICs), designated by their Secretary or agency head, are the highest ranking individuals within a federal department or agency that serve as the primary liaisons between the respective departments or agencies and the IC. Designation of FSICs at Executive Branch departments and agencies, which began in 2012, assists in defining responsibilities and moving toward true intelligence integration.

U.S. INTELLIGENCE COMMUNITY

The IC consists of 17 Executive Branch agencies and organizations that conduct intelligence and counterintelligence activities in support of U.S. foreign policy and the protection of our national security. Intelligence informs policy decisions, military actions, international negotiations, and interactions with foreign countries. IC elements that have a global emphasis make significant contributions to our homeland security and defense. Intelligence from these organizations in the form of alerts, warnings, notifications, and other reporting is shared in accordance with appropriate safeguards primarily through DHS/I&A and the FBI to domestic enterprise customers and partners.

The organizations described below serve as primary gateways for appropriate IC engagements with FSLTT partners (e.g., serving as integration points for sharing through the FSLTT intersection points described above, task force participation, and the exchange of staff officers and analysts with HS&LE organizations).

DHS

DHS is responsible for the unified national effort to secure the U.S. by preventing and deterring terrorist attacks and responding to other threats and hazards. It also has statutory responsibilities to provide threat information to the owners and operators of critical infrastructure and key resources. DHS/I&A provides intelligence support across the full range of homeland security missions. DHS/I&A ensures that information related to homeland security threats is collected, analyzed, and disseminated to all relevant customers across the domestic enterprise. The DHS Under Secretary for I&A also serves as their Chief Intelligence Officer and reports to both the Secretary of DHS and the DNI.

See Something Say Something campaign, provided by DHS

DHS/I&A has a unique mandate within the IC for sharing information and serving as an information conduit and intelligence advocate for state, local, tribal, and territorial governments. DHS/I&A supports fusion centers with deployed personnel and SECRET-level systems, security clearances, training, technical assistance, exercise support, and collaboration.

This National Network of Fusion Centers is the hub of much of the two-way intelligence and information flow among the FSLTT partners. Fusion centers represent a shared commitment between the federal government and the state and local governments who own and operate them. DHS/I&A officers report and disseminate information of intelligence value from DHS components, FSLTT partners, and open source collection to the IC and the DHS Intelligence Enterprise. DHS/I&A also supports statutory responsibilities to provide terrorism, cyber, and other threat information to the owners and operators of critical infrastructures and key resources.

Several other DHS component agencies have regular interaction with the IC, including Immigration and Customs Enforcement (ICE), Customs and Border Protection (CBP), Transportation Security Administration (TSA), U.S. Secret Service (USSS), and U.S. Citizenship and Immigration Services (USCIS).

FBI agents arresting a suspect, photo provided by FBI

FBI

The FBI's ability to leverage law enforcement and intelligence capabilities is critical to protecting the homeland. The FBI has the lead domestic role in investigating international terrorist threats to, and in conducting counterintelligence activities to meet foreign entities' espionage and intelligence efforts directed against, the U.S. The FBI is also responsible for coordinating collection of foreign intelligence and counterintelligence activities with other IC elements inside the U.S., and leads the IC effort to integrate intelligence support in the domestic field through the DNI Representative (DNI Rep) program. The FBI is able to execute these roles because, under applicable statutes and Executive Order 12333, it can exercise a broader range of domestic activities than other intelligence agencies. The FBI can also leverage the capacities of its 56 field offices, supporting FIGs, JTTFs, cyber teams, and criminal authorities to support its efforts. A critical force multiplier for the FBI is its engagement in over 400 national security and criminal task forces with FSLTT partners and its participation in the National Network of Fusion Centers. The JTTF is an example of active partnership. The 104 JTTFs are multi-jurisdictional task forces established to conduct terrorism-related investigations. JTTF investigations are focused on known threat actors or identified individuals who meet the thresholds under the Attorney General Guidelines for domestic FBI operations. Using the information derived from FBI FIGs, JTTFs, and fusion centers, the FBI develops intelligence products on significant developments or trends related to terrorism. These intelligence products may be used by partners to support their law enforcement and homeland security activities, such as intelligence-led policing efforts, implementing protective measures, or other target-hardening initiatives.

FIGs are located in each of the FBI's 56 field offices and are staffed with FBI intelligence analysts, language analysts, and special agents who provide domain awareness for their areas of responsibility (AOR) and complement the overall FBI analytic effort. FIGs are the primary mechanism through which FBI field offices develop human intelligence, identify emerging trends, and identify, evaluate, and prioritize threats within their AORs. They support domain awareness and investigative efforts through the use of strategic and tactical analysis, linguists, subject matter experts, special operations groups, and specialized surveillance groups. FIGs have established processes for collecting, analyzing, and producing intelligence information. These processes enhance the nation's ability to successfully penetrate national and transnational criminal networks, terrorist organizations, foreign intelligence services, and other entities that seek to harm the U.S. FIGs may also disseminate information to the IC and other federal, state, local, and tribal agencies, as well as foreign counterparts. Utilizing dissemination protocols, FIGs contribute to local and regional perspectives on all threats, and serve as the FBI's primary intelligence link with fusion centers.

The Terrorist Screening Center (TSC) serves as the USG's consolidation point for known and suspected foreign and domestic terrorist watch list information. The consolidated watch list contains thousands of records that are updated daily and shared with FSLTT law enforcement, IC members, and select international partners to ensure that individuals with links to terrorism are appropriately screened. The TSC, which is administered by the FBI and supported by federal departments and agencies, including DOJ, DHS, the Department of State (DoS), the ODNI, and the National Counterterrorism Center (NCTC), ensures that information provided to and consolidated by TSC is thorough, current, and accurate.

DEA

DEA is the lead federal agency for the enforcement of controlled substances laws and regulations of the U.S. It brings to the criminal and civil justice system those organizations and principal members of organizations involved in the cultivation, manufacturing, or distribution of controlled substances appearing in or destined for illicit traffic in the U.S., and supports non-enforcement programs aimed at reducing the availability of illicit controlled substances on the domestic and international markets.

DEA has 226 domestic offices and its workforce is supplemented with nearly 2,500 domestic police officers that are deputized as DEA task force agents. These agents, working under DEA supervision, are authorized to enforce federal laws and are the cornerstone of DEA's interaction with state and local law enforcement. DEA coordinates drug intelligence worldwide to assist in disrupting or dismantling international drug trafficking organizations. DEA maintains both a global and domestic presence, and ensures that a clear bridge exists between the two.

The DEA intelligence program works to provide predictive intelligence to identify trends and vulnerabilities in order to guide and prioritize the application of limited enforcement resources. The Office of National Security Intelligence (ONSI) was designated a member of the IC in February 2006. The objective of ONSI is to maximize DEA's contribution to national security, while protecting the primacy of its law enforcement mission.

Domestically, DEA shares intelligence with appropriate FSLTT agencies at multiple stages and at multiple points. Initial sharing of information occurs through direct contact with the partners. Each DEA field division and district office maintains a presence on the local JTTF, providing a direct conduit for sharing. Outside of the JTTF, information is shared directly with the responsible agency and/or through the HIDTAs and fusion centers. Additionally, DEA task force officers offer a direct link to their parent departments and agencies. Concurrently, relevant information is shared at the national level via the ONSI and the Special Operations Division, ensuring that information obtained by DEA is shared across multiple tracks with all relevant customers and partners.

Department of the Treasury

Treasury is the department responsible for promoting economic prosperity and ensuring the financial security of the U.S. Treasury. It is responsible for a wide range of activities, such as advising the President on economic and financial issues, encouraging sustainable economic growth, and fostering improved governance in financial institutions. Treasury works with other federal agencies, foreign governments, and international financial institutions to encourage global economic growth, raise standards of living,

Seizure by the Drug Enforcement Administration, photo provided by DEA

and, to the extent possible, predict and prevent economic and financial crises. Treasury also performs a critical and far-reaching role in enhancing national security by implementing economic sanctions against foreign threats to the U.S., identifying and targeting the financial support networks of national security threats, and improving the safeguards of the country's financial systems. Created under the Intelligence Authorization Act of 2004, the Office of Intelligence and Analysis (OIA) is Treasury's IC component. OIA officers help draft Treasury policy and support the execution of Treasury's regulatory and enforcement authorities by providing all-source intelligence analysis. Often, traditional intelligence is integrated with financial intelligence generated by administrative, law enforcement, and private sector partners. OIA also supplements intelligence support provided by DHS to the Treasury Department in its role as the financial-sector agency for critical infrastructure protection.

USCG

As the principal federal agency responsible for maritime safety, security, and stewardship, the USCG protects vital economic and security interests of the U.S. and has strong partnerships with FSLTT entities. In addition to its responsibility for the safety and security of the maritime public, the maritime transportation system, and the integrity of maritime borders, the USCG fills a unique niche in the IC. USCG intelligence provides timely and actionable intelligence and criminal investigative expertise to support tactical and operational commanders, strategic planners and leaders, and to meet national and homeland security intelligence requirements. As a result of its diverse authorities and mission areas, the USCG maintains broad awareness of the maritime environment.

USCG vessel, photo provided by USCG

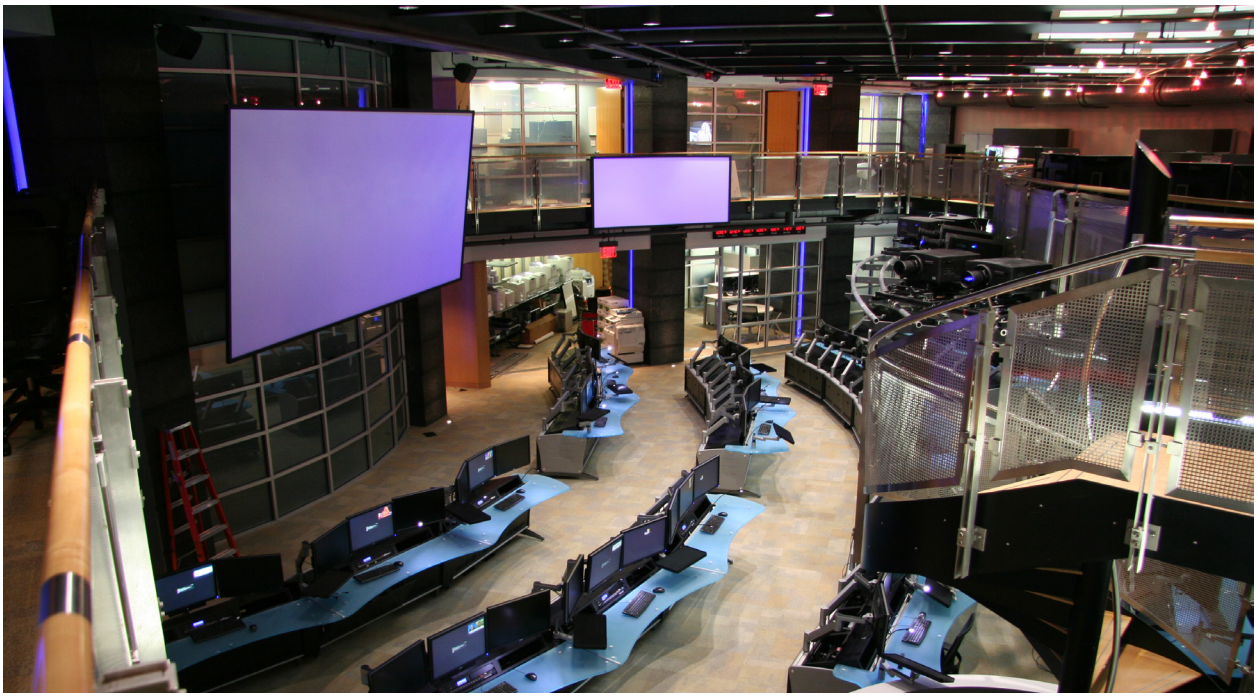
SUPPORTING DOMESTIC INTEGRATION

The following ODNI components are tasked with supporting and improving intelligence integration in the domestic field:

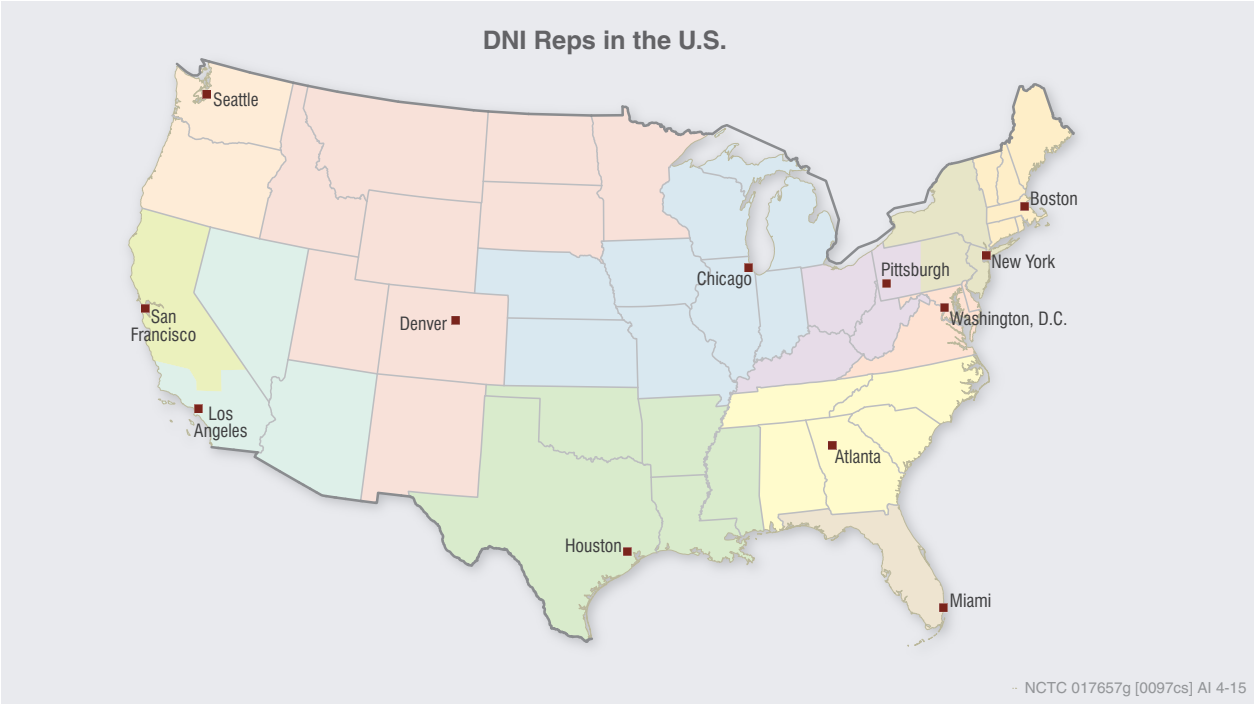
NCTC

NCTC has primary responsibility within the USG for analysis and integration of all intelligence possessed or acquired by the USG pertaining to terrorism and counterterrorism, excepting intelligence pertaining exclusively to domestic terrorists and domestic counterterrorism. NCTC executes these duties through efforts in intelligence analysis, information sharing, counterterrorism strategic operational planning, and maintaining the USG's central repository of identities information for known or suspected terrorists in support of the USG's terrorist screening process.

Supporting the counterterrorism mission is the NCTC-led Joint Counterterrorism Assessment Team (JCAT), which replaced the Interagency Threat Assessment and Coordination Group (ITACG) in April 2013. Its mission is to improve information sharing and enhance public safety. In coordination with the FBI and DHS, JCAT collaborates with other members of the IC to research,



NCTC Operations Center, provided by NCTC



produce, and disseminate counterterrorism intelligence products for FSLTT partners, and advocates for the counterterrorism intelligence requirements and needs of these partners throughout the IC. JCAT aims to improve the quantity and quality of intelligence products for FSLTT partners. Like ITACG, JCAT is located within NCTC and is composed of fully cleared state, local, and tribal HS&LE partners, as well as representatives from NCTC and its federal partners, DHS and FBI.

NCTC maintains the Terrorist Identities Datamart Environment (TIDE), which is the USG's central and shared knowledge bank on known or suspected international terrorist identities. NCTC also has the unique mission to be the two-way interface between domestic law enforcement and homeland security apparatus and the IC for terrorist identity and encounter information. NCTC is the single point of national integration for information sharing regarding terrorist identity data through the TIDE database. It provides selected exports of terrorist identity information to U.S. domestic screening and border entities through the TSC.

Additionally, NCTC's domestic representatives are uniquely equipped to facilitate the flow of both strategic and regional counterterrorism information to and from NCTC. They are primarily co-located with DNI Reps and strive to share counterterrorism-related intelligence with federal, state, local, and tribal personnel, always working via their FBI and DHS counterparts.

NCSC

The National Counterintelligence and Security Center (NCSC), previously known as the Office of the National Counterintelligence Executive, was established to help counter threats from foreign adversaries who seek to acquire national defense information, undermine the country's economic and technological advantage, and influence governmental processes. NCSC facilitates the enhancement of U.S. counterintelligence activities by: 1) enabling the counterintelligence community to fulfill its mission of identifying, assessing, prioritizing, and countering the intelligence threats to the U.S.; 2) ensuring that the counterintelligence community acts in an efficient and effective manner; and 3) providing for the integration of all counterintelligence activities.

Cyber Threat Intelligence Integration Center (CTIIC)

In February 2015, the President directed the DNI to establish the CTIIC to support the federal government's efforts to anticipate, mitigate, and counter foreign cyber threats to the U.S. and our national interests. CTIIC supports the federal cyber community—including cybersecurity centers, the IC, other relevant departments and agencies, and senior policymakers. It facilitates the timely information sharing of threat intelligence and related indicators, integrates analysis of threat trends and events, identifies gaps in knowledge, and helps the community identify opportunities to degrade or mitigate threat capabilities.

DNI Representatives in the U.S.

Leveraging 12 senior FBI officials across the U.S., the primary mission of the DNI Rep is to lead IC efforts within his or her AOR by creating an IC enterprise that is coordinated, integrated, agile, and effective. The role of a DNI Rep is to engage and periodically convene U.S. senior field representatives of each IC element in their respective AOR. DNI Reps conduct coordinated outreach to ensure that appropriate entities are aware of the IC's capabilities, analytic products, and resources while facilitating and monitoring implementation of DNI direction, policies, and procedures. This single-enterprise approach integrates intelligence in defense of the homeland and supports U.S. national security interests at home and abroad.

National Intelligence Manager (NIM) for the Western Hemisphere and the Homeland (NIM-WHH)

The NIM for the Western Hemisphere and the Homeland is responsible for partnering closely with other functional and regional NIM teams, ODNI/Partner Engagement, and DNI Reps to ensure FSLTT equities (e.g. homeland security information, criminal intelligence, etc.) are identified and considered at the national intelligence level. The Unifying Intelligence Strategy (UIS) for the Western Hemisphere serves as a key instrument for integrating the efforts of the IC in support of the Western Hemisphere, which includes the U.S. homeland. The UIS identifies opportunities and priorities for intelligence integration in support of IC and FSLTT partners where foreign intelligence affects FSLTT information, and vice versa.

U.S.-Mexico Border, photo provided by CBP

National Maritime Intelligence-Integration Office (NMIO)

NMIO's mission is to advance maritime intelligence integration, information sharing, and domain awareness to foster unity of effort for decision advantage that protects the United States, its allies and partners against threats in or emanating from the global maritime domain. NMIO serves as the nexus for the Global Maritime Community of Interest (GMCOI) to improve collaboration and facilitate integration, while keeping the highest levels of the U.S. Government informed on maritime information issues.

Program Manager for the Information Sharing Environment

PM-ISE is designed with one key goal in mind: to combat terrorism more effectively. The Intelligence Reform and Terrorism Prevention Act (2004) established an Information Sharing Environment (ISE), which is managed by the Program Manager for the ISE and comprises policies, procedures, and technologies linking the resources (people, systems, databases, and information) of FSLTT entities to facilitate terrorism information sharing, access, and collaboration.

PM-ISE has a government-wide mandate to facilitate the sharing of information with regard to terrorism, weapons of mass destruction, and homeland security in a manner consistent with national security and applicable legal standards relating to privacy and civil liberties. PM-ISE is working to achieve discrete, coordinated, and focused efforts leading to the delivery of interoperable, reused, and in some cases shared agency capabilities to accelerate mission impact.

DOD

DoD's role can be summarized as follows: 1) homeland defense - the protection of U.S. territory, its domestic population, and critical defense infrastructure against external threats and aggression; and 2) civil support - providing military support to civil authorities at the federal, state, and local levels across a range of conditions. The Secretary of Defense describes the three circumstances under which DoD assets could be involved in homeland defense and civil support missions as follows:

In extraordinary circumstances, DoD would conduct military missions such as combat air patrols or maritime defense operations. DoD would take the lead in defending the people and the territory of our country, supported by other agencies. Included in this category are cases in which the President, exercising constitutional authority as Commander-in-Chief and Chief Executive, authorizes military action to counter threats within the U.S.

In emergency circumstances, such as managing the consequences of a terrorist attack, natural disaster, or other catastrophe in support of civil authorities, DoD could be asked to act quickly to provide capabilities that other agencies do not possess or that have been exhausted or overwhelmed.

In non-emergency circumstances of limited scope or planned duration, DoD would support civil authorities where other agencies have the lead—for example, providing security at a special event such as the Olympics, or assisting other federal agencies to develop capabilities to detect chemical, biological, nuclear, and radiological threats.

DoD cannot provide for all aspects of homeland security. The homeland security mission requires the use of the full range of political, economic, diplomatic, and military tools, including enhanced intelligence to improve potential detection of future attacks. Domestic law enforcement agencies will bear a heavier burden in meeting domestic security needs. In addition, emergency preparedness planning and capabilities, which integrate the strengths of federal, state, and local authorities, are the first lines of response and defense in the homeland. Much of homeland security will entail localized responses, supported by planning and coordination with other levels of government.

U.S. Northern Command (USNORTHCOM)

USNORTHCOM's mission is to conduct homeland defense (protection against external threats and aggression), civil support, and security cooperation to defend and secure the U.S. and its interests. Its primary area of operation includes air, land, and sea approaches and encompasses the continental U.S., Alaska, Canada, Mexico, and the surrounding water out to approximately 500 nautical miles. It also includes the Gulf of Mexico, the Straits of Florida, and portions of the Caribbean region to include the Bahamas, Puerto Rico, and the U.S. Virgin Islands.

The Commander of USNORTHCOM also commands North American Aerospace Defense (NORAD) Command, a combined U.S.-Canadian team responsible for aerospace warning, aerospace control, and maritime warning for Canada, Alaska, and the continental U.S. In conjunction with its other missions, NORAD assists in the detection and monitoring of merchant vessels and aircraft suspected of illicit trafficking. This information is passed to civilian law enforcement agencies to help combat the flow of contraband into North America.

Military jet conducting a patrol exercise, photo provided by DoD

Joint Task Force North (JTF North), a subcomponent of USNORTHCOM, is the DoD organization tasked to support our nation's federal law enforcement agencies in the interdiction of suspected transnational threats within and along the approaches to the continental U.S. Transnational threats comprise activities conducted by individuals or groups that involve international terrorism, cyber threats, narcotics trafficking, alien smuggling, weapons of mass destruction, and the delivery systems for such weapons that threaten the national security of the U.S. JTF North support to federal law enforcement agencies is organized into the following six categories: intelligence, operational, engineering, general, interagency synchronization, and technology integration. Within the intelligence support category, JTF North provides the following: agency case-sensitive intelligence support, collaborative threat assessments, geospatial intelligence support, modified threat vulnerability assessments, and threat link analysis products.

Other Key Considerations

SECURITY CLEARANCE REFORM

The ability to share classified information across the domestic enterprise at the SECRET-level, between the IC and FSLTT partners, is critical for effective intelligence integration. A key enabler to support this requirement is a streamlined process for nominating, investigating, adjudicating, granting, and tracking security clearances for partner agencies. Security clearance reform set the conditions for great progress over the last five years. In August 2010, Executive Order 13549, "Classified National Security Information Program for FSLTT entities", designated the Secretary of Homeland Security as the Executive Agent for this effort. Working with the FBI and other federal partners, DHS established governance and an oversight structure to promote the uniform application of SECRET-level security clearance standards. Additionally, security liaison officers were designated at state and major urban area fusion centers to assist with nominations and the processing of security clearance requests. In 2006, the average processing time for initial security clearances was 165 days. Presently interim SECRET clearance determinations are made based on preliminary checks within 14 days of requests being received by the sponsoring agency. Final clearances are issued once the Office of Personnel Management completes its investigation and there is a favorable adjudication of the request. The average processing time in 2015 for a final SECRET clearance was 116 days. DHS and FBI currently hold over 10,000 SLTT and private sector clearances.

NATIONAL STRATEGY FOR INFORMATION SHARING & SAFEGUARDING

Our national security depends on the ability to share the right information, with the right people, at the right time. This information sharing mandate requires sustained and responsible collaboration between the IC and FSLTT partners. Over the last few years, the IC and FSLTT partners have successfully streamlined policies and processes, overcome cultural barriers, and better integrated information systems to enable information sharing. Today's dynamic environment, nonetheless, poses challenges to the continuing effort to improve information sharing and safeguarding processes and capabilities. While innovation has enhanced the ability to share, increased sharing has created the potential for vulnerabilities that require strengthened safeguarding practices. The 2012 National Strategy for Information Sharing and Safeguarding provides guidance for effective development, integration, and implementation of policies, processes, standards, and technologies to promote secure and responsible information sharing. The strategy does not define particular categories or types of information that must be shared. Rather, it shifts the focus of information sharing and safeguarding policy to defining information requirements that support effective decision making. The strategy outlines a vision with a national policy roadmap to guide information sharing and safeguarding within existing law and policy. This strategy does not replace the National Strategy for Information Sharing (2007 NSIS), as the 2007 NSIS continues to provide a policy framework and directs many core initiatives intended to improve information sharing.

Way-Ahead

This paper promotes a better understanding of the current operating environment of the domestic enterprise. Going forward, it will be important to move beyond the "as is" descriptions and work toward a vision of the "should be." This vision must guide long-term investment strategies that align assets to better synchronize intelligence collaboration and interplay with FSLTT partners, while ensuring the privacy, civil rights, and civil liberties of our citizens are fully protected. It must also help to identify potential changes to policies, technologies, and organizational and informational frameworks to optimize both cost and effectiveness. Ultimately, the domestic enterprise must be postured to provide all-source intelligence and enhance responsible information sharing and collaboration across public safety, law enforcement, and intelligence activities. This will ensure that our customers and partners—from first responders to our national leaders—have the most accurate and current intelligence.

Abbreviations

AOR	Area of Responsibility
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
CAC	Civil Applications Committee
CBP	Customs and Border Protection
CI	Counterintelligence
CIA	Central Intelligence Agency
CICC	Criminal Intelligence Coordinating Council
CIU	Criminal Intelligence Unit
CT	Counter Terrorism
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DHS/I&A	Department of Homeland Security Office of Intelligence & Analysis
DIA	Defense Intelligence Agency
DNI	Director of National Intelligence
DoD	Department of Defense
DoJ	Department of Justice
DoS	Department of State
DOT	Department of Transportation
EMS	Emergency Medical Services
FBI	Federal Bureau of Investigation
FICO	Federal Intelligence Coordination Office
FIG	Field Intelligence Group
FSIC	Federal Senior Intelligence Coordinator
FSLTT	Federal, state, local, tribal, and territorial
HHS	Health and Human Services
HIDTA	High Intensity Drug Trafficking Area
HIFCA	High Intensity Financial Crime Area
HSA	Homeland Security Advisor
HS&LE	Homeland Security & Law Enforcement
IC	Intelligence Community
ICE	Immigration and Customs Enforcement
IIR	Intelligence Information Report
INR	Bureau of Intelligence and Research
ISC	Investigative Support Center
ITACG	Interagency Threat Assessment and Coordination Group
JCAT	Joint Counterterrorism Assessment Team
JTF	Joint Task Force
JTTF	Joint Terrorism Task Force
LE	Law Enforcement
NCSC	National Counterintelligence and Security Center
NCTC	National Counterterrorism Center
NGA	National Geospatial-Intelligence Agency
NIM	National Intelligence Manager
NORAD	North American Aerospace Defense
NORTHCOM	Northern Command
NRO	National Reconnaissance Office
NSA	National Security Agency
NSI	Nationwide Suspicious Activity Reporting Initiative
NSIS	National Strategy for Information Sharing
ODNI	Office of the Director of National Intelligence
OIA	Office of Intelligence and Analysis, Treasury Department
ONDCP	Office of National Drug Control Policy
ONSI	Office of National Security Intelligence
OPM	Office of Personnel Management
PM-ISE	Program Manager for the Information Sharing Environment
RISS	Regional Information Sharing System
SAR	Suspicious Activity Report
SBU	Sensitive But Unclassified
TIDE	Terrorist Identities Datamart Environment
TSA	Transportation Security Administration
TSC	Terrorist Screening Center
TTP	Tactics, Techniques and Procedures
UIS	Unifying Intelligence Strategy
USCG	U.S. Coast Guard
USCIS	U.S. Citizenship and Immigration Services
USG	U.S. Government
USGS	U.S. Geological Survey
USSS	U.S. Secret Service

Domestic Approach to National Intelligence

Domestic Enterprise


ME
Augusta
Montpelier
VT
NH
Concord
Boston
MA
Albany
NY
Buffalo
CT
Hartford
RI
Providence
MI
Lansing
Detroit
PA
Harrisburg
Trenton
NJ
Pittsburgh
Cleveland
Dover
MD
DE
Annapolis
WASHINGTON, D.C.
IN
OH
Columbus
Cincinnati
WV
Charleston
VA
Richmond
Louisville
Frankfort
KY
London
Raleigh
NC
Knoxville
Charlotte
TN
pending
Columbia
SC
Atlanta
Birmingham
AL
GA
Montgomery
Jacksonville
Tallahassee
FL
Orlando
Tampa
Miami
AK
Anchorage
Juneau
San Juan
PR
Charlotte Amalie
VI
VT
NH
pending
Boston
Albany
NY
MA
Providence
Hartford
CT
RI
New Haven
Newark
New York City
PA
Philadelphia
Trenton
Harrisburg
NJ
Baltimore
Dover
MD
DE
Annapolis
WASHINGTON, D.C.
VA
Richmond
Norfolk
0
100 Kilometers
0
100 Miles

This Page was Intentionally Left
BLANK

This Page was Intentionally Left
BLANK

This Page was Intentionally Left
BLANK

UNITED TO PROTECT

★ ★ ★ ★

NCTC 029197 | December 2016