# Guideline 2 – Develop a Common Framework for the Sharing of Information Between and Among Executive Departments and Agencies and State, Local, and Tribal Governments, Law Enforcement Agencies, and the Private Sector

## I. Introduction

In the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Congress directed the establishment of an Information Sharing Environment (ISE) to improve and facilitate the sharing of terrorism information. On December 16, 2005, and in furtherance of his efforts to implement the enactment, the President issued a Memorandum for the Heads of Executive Departments and Agencies, which establishes guidelines and directs particular actions to effect the creation and operation of the ISE.

Guideline 2 of the President's Memorandum directed the development of "a Common Framework for the Sharing of Information Between and Among Executive departments and Agencies and State, local, and tribal Governments, Law Enforcement Agencies, and the Private Sector." Specifically, Guideline 2 directed the Attorney General and the Secretary of Homeland Security, in consultation with the Secretaries of State, Defense, and Health and Human Services and the Director of National Intelligence, to:

> (i) perform a comprehensive review of the authorities and responsibilities of executive departments and agencies regarding information sharing with State, local, and tribal governments, law enforcement agencies, and the private sector; and
>
> (ii) submit to the President for approval, through the [Assistant to the President for Homeland Security and Counterterrorism] APHS-CT and the [Assistant to the President for National Security Affairs] APNSA, a recommended framework to govern the roles and responsibilities of executive departments and agencies pertaining to the acquisition, access, retention, production, use, management, and sharing of homeland security information, law enforcement information, and terrorism information between and among such departments and agencies and State, local, and tribal governments, law enforcement agencies, and private sector entities.

In response to the President's directive, the Department of Justice (DOJ) and Department of Homeland Security (DHS), with assistance from the Office of the Program Manager for the Information Sharing Environment (PM-ISE), have proposed such a framework for information sharing. This document delineates that framework by outlining the principles that guided the construction of the framework, explaining the framework's

essential requirements, and committing all participating agencies to an implementation and monitoring plan.

The proposed framework draws upon existing systems and capabilities and mandates a coordinated and collaborative approach to sharing homeland security information, terrorism information, and law enforcement information with State, local, and tribal officials and the private sector. The proposed framework will enable more effective and efficient sharing of this information both at the Federal level (between and among departments and agencies) and with State, local, and tribal governments and private sector entities. The framework has been designed to enable the achievement of practical solutions to any logistical challenges that surface in the framework's operation and, more generally, along the road to implementing the ISE.

## II. Process Used to Complete Task

The Attorney General and the Secretary of Homeland Security directed action to develop a framework and governance model for the acquisition, access, retention, production, use, management, and sharing of the information addressed in Guideline 2. DOJ and DHS established an interagency working group to respond to the President's directives. Interagency sub-working groups then undertook efforts to examine certain relevant issues, including the identification of legal authorities pertinent to Guideline 2's directives. Other efforts focused on establishing policies and procedures to govern the dissemination of unevaluated domestic threat reporting and the effective production of tear line reports. Still other efforts evaluated the use and production of national security related information within the classified domain insofar as it is relevant to the activities as described in Guideline 2. Input from certain non-federal partners was solicited through a meeting of the State, local, and tribal Subcommittee of the Information Sharing Council. Furthermore, consultation was undertaken with other Federal departments both directly and through the Information Sharing Council.

In devising the proposed framework, participants evaluated for effectiveness the current environment in which information sharing occurs. They also identified potential gaps and areas of improvement. Additionally, to ensure consistency and accuracy, they defined key terms and specific functions relating to information sharing. Finally, they reached agreement on the key principles guiding the information sharing framework. Based on all of these activities, they developed specific findings and recommendations (see Section VI).

Collectively, these processes have resulted in the development of a proposed framework that embodies a vision for information sharing that maximizes the opportunity for success and does not encumber participation with impediments of location, classification, organizational boundaries, or cultures.

## III. Information Sharing – the Current Environment

The information sharing framework currently in place does not sufficiently coordinate the sharing of terrorism information between and among Federal and State, local, and tribal entities and the private sector. A better framework is necessary because the counterterrorism roles and responsibilities of these entities often intersect and overlap. In the current environment, multiple communications channels, processes, and systems are used at the Federal level to address various aspects of sharing terrorism information. The lack of a systemic and coordinated approach to sharing terrorism information can result in the production and dissemination of mixed and at times competing messages from Federal officials. Furthermore, there is a lack of clarity regarding the Federal government's expectations of State, local, and tribal officials in the area of State and local reporting of terrorism information. This lack of clarity has limited the Federal government's ability to receive information from State and local officials. A robust information sharing framework is necessary to address and resolve these deficiencies and to empower all participating Federal entities to undertake a collaborative and coordinated approach to sharing terrorism information with State, local, and tribal officials.

Homeland security information, terrorism information, and law enforcement information can be found across all levels of government as well as in the private sector. Successful counterterrorism efforts require that Federal, State, tribal, local, and private-sector entities have an effective information sharing capability.

The process undertaken to construct the proposed framework revealed that State, local, and tribal governments use national security-related information for multiple purposes. Those purposes include not only undertaking law enforcement initiatives, but also efforts to determine the allocation of funding and other resources for homeland security-related purposes; develop critical infrastructure protection and resiliency plans; prioritize emergency management, response, and recovery planning activities; devise training and exercise programs; and support efforts to prevent terrorist attacks. Accordingly, at the State, local, and tribal level, homeland security activities often include participation by both law enforcement and non-law enforcement personnel, including public health, transportation, emergency management, fire, emergency medical, and public works entities.

It is therefore essential that the proposed information sharing framework be designed and able to:

a. Achieve greater awareness of information needs and requirements between and among Federal, State, local, and tribal officials and private sector domains;

b. Allow for an authoritative, coordinated response and communication across Federal, State, local, tribal and private sector domains; and

c. Ensure that the Federal information sharing environment meets and interacts effectively with State, local, and tribal sharing environments, including, for example, State fusion centers.

## IV. Framework Definitions and Specific Information Sharing Functions

### *Definitions*

Guideline 2 requires the construction of a framework for "homeland security information," "terrorism information," and "law enforcement information." There is overlap among these terms. For purposes of constructing and implementing the framework required by Guideline 2, it is not necessary to delineate the precise contours of the definitional overlap. The definitions are set out below to identify, by category, the information addressed by Guideline 2 and to make plain that the terms are being used here only in the context of their applicability to national security matters in the terrorism arena. The definitions are not intended to explain or catalogue any particular department or agency's authority, or lack thereof, to perform a certain function or undertake a certain activity as part of protecting our homeland and/or preventing, deterring, or responding to a terrorist act. To the extent necessary, those roles and responsibilities are addressed in other portions of this document.

Accordingly, for purposes of the framework established in this document, the following definitions apply:

"Homeland security information," as defined in Section 482(f)(1) of the Homeland Security Act , means any information possessed by a Federal, State, local, or tribal agency that relates to (A) a threat of terrorist activity; (B) the ability to prevent, interdict, or disrupt terrorist activity; (C) the identification or investigation of a suspected terrorist or terrorist organization or any person, group, or entity associated with or assisting a suspected terrorist or terrorist organization; or (D) a planned or actual response to a terrorist act.

"Terrorism information," as defined in Section 1016(a)(4) of IRTPA means all information relating to (A) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism; (B) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations; (C) communications of or by such groups or individuals; or (D) groups or

individuals reasonably believed to be assisting or associated with such groups or individuals.

For purposes of the ISE, "law enforcement information" means any information obtained by or of interest to a law enforcement agency or official that is both (A) related to terrorism or the security of our homeland and (B) relevant to a law enforcement mission, including but not limited to information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counterterrorism investigation; assessment of or response to criminal threats and vulnerabilities; the existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct; the existence, identification, detection, prevention, interdiction, or disruption of, or response to, criminal acts and violations of the law; identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and victim/witness assistance.

### *Functions*

The framework required by Guideline 2 pertains to specified functions, namely the "acquisition, access, retention, production, use, management, and sharing" of homeland security, law enforcement, and terrorism information. Accordingly, it is prudent that a common understanding exist as to the meaning of these functions. The following descriptions, which are provided only for purposes of this document, are designed to guide the implementation and operation of the framework. The descriptions are followed by a perspective on how these functions manifest themselves in the Federal-to-Federal and Federal-to-State, local, and tribal and private sector domains.

ACQUISITION refers to the means by which an ISE participant obtains information through the exercise of its authorities, for example, through human intelligence collection or from a foreign partner. For the purposes of this definition, acquisition does not refer either to the obtaining of information widely available to other ISE participants through, for example, news reports, or to the obtaining of information shared with them by another ISE participant who originally acquired the information.

> Federal-to-Federal: The acquisition of homeland security information, terrorism information, and law enforcement information occurs as a direct result, or by-product, of activities carried out by several Federal departments and agencies. Existing authorities provide an ample and appropriate basis to guide the original acquisition of information.

Federal-to-State, local, and tribal officials/Private Sector: Similarly, the acquisition of information at the State, local, and tribal level and by private sector entities is governed by a variety of laws, policies, and business practices. Over time best practices for managing the acquisition of information will emerge at all levels of government across the country. As the ISE operates, its participants should draw upon these best practices to assist in refining acquisition processes.

ACCESS refers to the business rules, means, and processes by and through which ISE participants obtain homeland security information, terrorism information, and law enforcement information acquired in the first instance by another ISE participant. As part of implementing the Guideline 2 framework, and in coordination with measures undertaken to establish the ISE, all participants should take steps to ensure that access controls are calibrated to achieve maximum information sharing while also providing appropriate security to classified or otherwise sensitive data and achieving compliance with privacy and other applicable laws.

Federal-to-Federal: At the Federal level, access to homeland security information, terrorism information, and law enforcement information is a function of several factors, including the interoperability of information network architectures, classification authorities and policies, the certification and accreditation of the security of information networks, personnel security requirements associated with sensitive, compartmented information, and the counterterrorism roles and responsibilities assigned to designated organizations. Governance structures are in place to address each of these categories. Accordingly, existing authorities are sufficient to govern access to terrorism-related information at the Federal level.

Federal-to-State, local, and tribal officials and the Private Sector: As the proposed framework operates, Federal officials will provide appropriate access to homeland security information, terrorism information, and law enforcement information to State, local, and tribal officials and private sector entities. In addition, the exchange of personnel between Federal and non-Federal entities can provide an effective means to extend appropriate and full access to data, without moving data into an environment where access controls and information management can create impediments.

RETENTION refers to the storage and safeguarding of homeland security information, terrorism information, and law enforcement information by both the originator of the information and any recipient of the information. Entities participating in information sharing governed by Guideline 2 must abide by existing authorities governing the retention and storage of information received from another party and, as appropriate, work in coordination and consultation with other parties to develop new and refined authorities to govern the retention and storage of information addressed by Guideline 2.

To ensure maximum information sharing and appropriate security, retention processes must be closely coordinated with those procedures governing access and use of information.

Federal-to-Federal: The retention of information is governed by the authorities under which Federal departments and agencies operate and the related purposes for which the information is acquired. Current retention policies or practices do not appear to impede the sharing of terrorism information.

Federal-to-State, local, and tribal officials/Private Sector: It is not clear that rules and practices regarding the retention of information that crosses between Federal, State, local, and tribal officials and private domains are sufficiently understood or documented to ensure the appropriate retention and disposition of information originating in one domain and passed to another through information sharing. Accordingly, this document contains a recommendation specifically tailored to achieving improvements in this area.

PRODUCTION refers to the dissemination and publication of homeland security information, terrorism information, and law enforcement information within the protocols established under the framework set forth in this document. Production efforts must focus not only on the substance of the information to be disseminated, but also on the form in which the information will be presented to our State, local, and tribal partners. While preserving existing production channels, the framework established in this document requires a collaborative and coordinated approach to production—all in an effort to speak with one voice to State, local, and tribal officials and private sector entities and thus to communicate, to the maximum extent possible, unified messages.

Federal-to-Federal: It is essential to recognize that information acquired for one purpose may serve many purposes, consistent with applicable law, and that information linked to a specific activity can have value to a broader community and can be perceived differently in the context of varied intended uses. Additionally, various Federal entities, including especially DOJ and DHS, share responsibility for preventing acts of terrorism and protecting the homeland. Accordingly, a coordinated and collaborative approach to production—leveraging the authorized capabilities, focus, and strength of each department—is necessary and essential if the Federal government is going to work effectively with State, local, and tribal officials and private sector entities.

Federal-to-State, local, and tribal officials and the Private Sector: The NCTC, in coordination with DOJ, DHS, and other Federal entities, will provide the Federal government's coordinated, integrated, and unified analytic judgments on terrorist threats to the homeland, and will support other departments and agencies in the

production of analytic material for sharing as appropriate with State, local, tribal, and private sector communities. This relationship is not intended to interfere with the activities of departments and agencies in conveying time-sensitive threat information in fulfillment of law enforcement, critical infrastructure protection, or public safety responsibilities.

USE refers to the actions or responses that recipients of homeland security information, terrorism information, or law enforcement information may take upon receiving such information acquired under their authorities or accessed from another ISE participant. The same piece of information can and often will be used for more than one purpose because many agencies and departments of government, including non-Federal governments, share responsibilities for preventing terrorism and protecting our Nation's security. The framework established by this document requires coordinated and collaborative production of terrorism-related information and thus is designed to enable effective and deconflicted use of the information.

Federal-to-Federal: At the Federal level, the goal should be to make the maximum amount of information possible available for use by recipients, consistent with applicable law. The National Implementation Plan, as approved by the President in June 2006, sufficiently defines the roles and responsibilities of Federal agencies and departments with counterterrorism obligations.

Federal-to-State, local, and tribal officials/Private Sector: As with retention, the rules and practices regarding the use of information that crosses between Federal, State, local, and tribal officials and private domains are not sufficiently understood or documented to ensure the appropriate disposition of information originating in one domain and passed to another through information sharing. Accordingly, this document contains a recommendation specifically tailored to achieving improvements in this area.

MANAGEMENT refers to the responsibility of an ISE participant to oversee and govern, as appropriate and applicable, its acquisition, access, retention, production, use, and sharing of homeland security information, terrorism information, and law enforcement information. In furtherance of the principles upon which the Guideline 2 framework has been constructed, management efforts should be designed to advance a coordinated and collaborative approach to information sharing.

Federal-to-Federal: At the Federal level, the management of homeland security information, terrorism information, and law enforcement information is presently inherent in roles and responsibilities articulated in statute, the National Implementation Plan, and agency practice and regulation, all of which impact upon the integration and use of information for analyses and assessment and for the

dissemination of intelligence products through the NCTC On Line secure web site. A coordinated and shared management approach, one that works effectively with State, local, and tribal officials, is essential to the proposed framework's operational success.

Federal-to-State, local, and tribal officials/Private Sector: In the aftermath of the September 11 attacks, State, local, and tribal entities have invested significant resources in managing terrorism-related information by, for example, establishing fusion centers. It is envisioned that State, local, and tribal officials, whether at fusion centers or elsewhere, will work effectively with their Federal counterparts.

SHARING refers to the act of one ISE participant disseminating or giving homeland security information, terrorism information, or law enforcement information to another ISE participant. The framework established by this document requires a coordinated and collaborative approach to information sharing and aims to maximize the quality and amount of the information shared while also appropriately safeguarding information and respecting individuals' privacy rights, civil liberties, and other legal rights protected by U.S. law.

Federal-to-Federal: At the Federal level, NCTC oversees a robust program for the sharing of terrorism information across the Federal intelligence, law enforcement, homeland security, defense, and foreign affairs communities.

Federal-to-State, local, and tribal officials/Private Sector: Responsibility for sharing information with State, local, tribal, and private sector entities will take place through existing channels. Federal assessments of threat and incident reporting will be conducted in a coordinated manner through the interagency group established in the sharing framework.

## V. The Proposed Framework

Federal, State, local, tribal and private sector authorities must share a common understanding of what information is needed to support efforts to prevent, deter, and respond to terrorist attacks. The common understanding will be achieved through a framework that enables:

- Federal entities to work more effectively in order to extend the sharing of information in ways that best address the information needs of State, local, tribal, and private sector partners;

- Federally generated information products to be disseminated more rapidly to State, local, tribal, and private sector entities; and

- Locally generated information to be efficiently gathered, processed, analyzed, and disseminated to Federal authorities.

### *Guiding Principles*

The following core principles guided the development of this framework and must inform its implementation:

- Effective information sharing comes through strong partnerships between and among Federal, State, local, and tribal authorities and private sector entities.

- Insofar as is consistent with applicable law, information acquired for one purpose or under one set of authorities may provide substantial value for understanding and uncovering unique insights when shared across multiple domains. Accordingly, there must exist a "culture of awareness" in which personnel at all levels of government understand that terrorism information is derived from multiple sources and used to support a variety of activities, including preventive and protective actions; immediate actionable response; criminal and counterterrorism investigative activities; event preparedness; and response to and recovery from catastrophic events.

- The procedures, processes, and systems that support information sharing must draw upon and integrate existing capabilities and must respect and give effect to existing authorities and responsibilities. Specifically, the framework must:

    - Protect and give effect to the Federal Bureau of Investigation's (FBI's) authority and responsibility to investigate terrorist activities and threats through its Joint Terrorism Task Forces (JTTFs), as well as its Field Intelligence Groups (FIGs), which provide corollary analytical support. Any law enforcement investigatory activity relating to terrorism undertaken by another participating entity must be coordinated with and through the JTTFs and FIGs.

    - Protect and give effect to DHS's authority and responsibility to share terrorism and related homeland security information with all relevant State, local, and tribal authorities and the private sector, as well as to provide them timely assessments of the threats of, risks from, and vulnerabilities to terrorism in support of preventive and protective actions designed to protect the homeland and manage the Federal government's preparedness for, and response to, incidents of terrorism.

    - Recognize that Federal agencies and departments carrying out their respective authorities, roles, and responsibilities must continue to share information with a broad range of State and local authorities. Accordingly, nothing in this

framework precludes any Federal government entities from having direct information sharing interaction with State, local, and tribal officials and private sector organizations in support of mission-specific and agency-specific activities insofar as such interactions are consistent with applicable law.

- State and major urban area fusion centers represent a valuable information-sharing resource and should be incorporated into the national information-sharing infrastructure. Effective integration will require that fusion centers achieve a baseline level of capability and comply with all applicable laws.

- While State, local, tribal, and private sector organizations require information that supports their mission responsibilities, it must be provided in such a way as to not compromise ongoing law enforcement investigations and intelligence operations.

- Activities undertaken within the framework must respect individuals' privacy rights, civil liberties, and other legal rights protected by U.S. laws.

- This information-sharing framework must be implemented without delay and participating Federal agencies should institute processes capable of continuously monitoring and refining its operation and structure.

### *Coordination at the Federal Level*

This framework is intended to serve both the ongoing exchange of information that will allow for discovery of emerging threats and risks and the enhancement of knowledge about existing threats and risks. The exchange of coordinated sets of requirements and information needs across the Federal and non-Federal domains will help guide more efficient and focused targeting, selection, and reporting of responsive information.

To better coordinate the sharing of terrorism information, the framework establishes an interagency threat assessment and coordination group at the national level (the "Group"). Within the Group the participants must engage in collaborative decision-making to ensure the timely and effective integration, vetting, sanitization, and communication of terrorism information across multiple agencies to inform and empower State, local, tribal, and private sector partners.

Consistent with the directives of Congress and the President to build upon existing systems and capabilities, the Group will be at the NCTC. The Secretary of Homeland Security will assign a senior official to manage and direct the day-to-day activities of the Group. Decision-making authority regarding how specific products will be disseminated to State, local, and tribal officials and the private sector will be primarily shared between DOJ and DHS and will include other agencies as appropriate. DOJ and DHS will lead an effort to develop standard operating procedures to govern how best to

integrate the activities of the Group with existing Intelligence Community production protocols. The Group will include representatives from the Department of Defense (DoD), DHS, FBI, and other relevant Federal entities.

The Group will facilitate the production of what will be officially defined as "Federally-Coordinated" terrorism information products intended for dissemination to State, local, and tribal officials and private sector partners. It will ensure that both classified and unclassified intelligence produced by Federal entities within the intelligence, law enforcement, and homeland security communities is fused, validated, deconflicted, and approved for dissemination in a concise and, where possible, unclassified format. When appropriate and practicable, reports disseminated to State, local, and tribal entities will contain suggested action items.

IRTPA assigns primary responsibility within the Federal government for analysis of terrorism information to NCTC. The statute also authorizes NCTC to support the Department of Justice and Department of Homeland Security and other appropriate agencies in fulfillment of their responsibilities to disseminate terrorism information. In fulfillment of this responsibility, NCTC is staffed by personnel from a wide variety of Federal departments and agencies, thus allowing the development of coordinated and integrated assessments of terrorist threats, plans, intentions, and capabilities. By co-locating a national coordination group with the NCTC, the Federal government can leverage this existing capacity and credibility in a mature environment that reflects experience in the complexities of interagency coordination and information exchange. This environment will provide direct access to Federal agencies represented at NCTC to rapidly effect decisions about sanitization and release of information that needs to be shared with State, local, and tribal officials and the private sector. Although collocated at the NCTC, the Group will not replicate or supplant the analytic or production efforts of the NCTC. Nor is it intended to duplicate, impede, or otherwise interfere with existing and established counterterrorism roles and responsibilities. The efforts of the Group are intended to complement and supplement existing analytic, production, and dissemination efforts by Federal entities.

Specifically, the Group will coordinate the production and timely issuance of the following interagency products intended for distribution to State, local, and tribal officials and the private sector:

- Alerts, warnings, notifications, and updates of time-sensitive information related to terrorism threats to locations within the United States;

- Situational awareness reporting regarding significant events or activities occurring at the international, national, State, or local levels (information regarding terrorism

investigative activity will continue to be disseminated to State, local, and tribal officials through the JTTFs or Field Intelligence Groups); and

- Strategic and foundational assessments of terrorist risks and threats to the United States and related trend and tradecraft information, including, for example, assessments of lessons learned from terrorist events or counterterrorism initiatives.

Products generated through the efforts of the Group will be disseminated through existing department and agency communication channels and systems. This framework, therefore, preserves existing channels of communication for each participating agency to use in fulfilling its agency-specific mandates in reporting to State, local, and tribal officials. Accordingly:

- The FBI will continue to be responsible for sharing with Federal and State, local, and tribal officials law enforcement personnel, and other relevant public and private entities, all terrorism information that supports its JTTFs' efforts to prevent, detect, disrupt, and defeat terrorist operations through the conduct of investigations of terrorist activity within the United States;

- DHS will continue to disseminate homeland security information to all State, local, and tribal officials authorities and relevant public and private sector entities in support of its mission to prevent terrorist attacks in the United States, reduce the overall vulnerability of the United States to terrorism, and undertake efforts to prepare for, protect against, respond to, and recover from terrorist activities against the homeland; and

- DoD will continue to provide to State and territorial National Guard units terrorism information to support force protection activities.

### *Integration and Role of the State and Major Urban Area Fusion Centers*

In the spirit of a federalist or shared-responsibility approach to information sharing, the Federal government will promote the establishment of a network of fusion centers to facilitate effective nationwide terrorism information sharing. The State and major urban area fusion centers will become the focus, but not exclusive points, within the State and local environment for the receipt and sharing of terrorism information. State, local, and tribal officials, as part of the implement of the framework, will be asked to identify the optimal interchange location(s) to meeting information sharing objectives. This approach will require State and major urban area fusion centers to achieve a baseline level of capability and to comply with all applicable privacy laws such as described by the recent Global/Homeland Security Advisory Council Fusion Guidelines—many of which have already been incorporated into the business processes of a number of existing fusion centers — or additional requirements that may be identified through

coordination between Federal, State, and local authorities. It is imperative that the State and urban area fusion centers understand and validate requests for information originating from the State, local, and tribal offices prior to submission to the Federal Government. The State and urban area fusion centers play an integral role in the timeliness of information dissemination and sharing through an active role in understanding and defining the State, local, and tribal requests for information.

The needs of State, local, and tribal entities continue to mount as they incorporate counterterrorism and homeland security activities into their day-to-day missions. Specifically, they need to ensure that personnel protecting local communities from terrorist attack—or responding to an attack—have access to timely, credible, and actionable information and intelligence regarding individuals and groups intending to carry out attacks within the United States, their organization and financing, at-risk potential targets, pre-attack indicators, and other major events or circumstances requiring action by State, local, and tribal officials.

It is important to note that Federal and State governments have a shared responsibility for ensuring the timely processing and dissemination of information to meet the needs of all end users. State and major urban area fusion centers can dramatically enhance efforts to gather, process, and share locally generated information regarding potential terrorist threats and to integrate that information into the analytical activities associated with understanding the national threat environment. Additionally, these centers can also coordinate the dissemination of terrorism information produced by Federal entities to State, local, tribal, and private sector entities in support of analytical, planning, and operational activities.

As participants in the ISE and the Guideline 2 sharing framework, State, local, and tribal entities should undertake the following activities and responsibilities, in appropriate consultation or coordination with Federal departments and agencies:

- Share information to address national security and criminal investigations in a manner that protects the privacy, civil liberties, and other legal rights of individuals protected by U.S. law, while ensuring the security of the information shared;

- Foster a culture that recognizes the importance of fusing "all crimes with national security implications" and "all-hazards" information (e.g., criminal investigations, terrorism, public health and safety, all-hazards and emergency response) and, often, involves capturing criminal activity and other information that might be a precursor to a terrorist plot;

- Support efforts to detect and prevent terrorist attacks by maintaining situational awareness of threats, alerts, and warnings;

- Develop critical infrastructure protection plans to ensure the security and resiliency of infrastructure operations (e.g., electric power, transportation, telecommunications, etc.) within a region, State, or locality;

- Prioritize emergency management, response, and recovery planning activities based on likely threat scenarios and at-risk targets;

- Determine the allocation of funding, capabilities, and other resources. This can take the form of prioritizing State, local, and tribal officials' funding, submitting Federal grants applications, and collocating Federal, State, local, and tribal assets; and

- Develop training, awareness, and exercise programs to ensure that State, local, and tribal officials personnel are prepared to deal with terrorist strategies, tactics, capabilities, and intentions, and to test plans for preventing, preparing for, mitigating the effects of, and responding to events.

In furtherance of their respective roles and responsibilities, Federal entities will share appropriate homeland security information, terrorism information, and law enforcement information with State and major urban area fusion centers. Unless specifically prohibited or subject to classification restrictions, State and major urban area fusion centers may further customize Federally supplied information for dissemination to meet intra- or interstate needs. In turn, it is essential that State and major urban area fusion centers ensure that all locally generated terrorism information—including suspicious activity/incident reports—is communicated consistent with applicable law to the Federal government through the appropriate mechanism and systems, which will be identified by Federal officials as part of the creation of the ISE. Locally generated information that is not threat or incident related will be gathered, processed, analyzed, and interpreted by the same State and major urban area fusion centers in coordination with locally-based Federal officials. The same information will be disseminated to the national level via the DoD, DHS, FBI, or other appropriate Federal agencies. Efforts should be made to accomplish this objective through the use of one or more centralized systems, appropriately available to State, local, and tribal partners.

### *Private Sector*

The private sector owns and operates over 80% of the nation's critical infrastructure and is therefore a primary source and repository for important vulnerability and other potentially relevant terrorism information. Accordingly, private sector information represents a crucial element both for understanding the current threat environment and

for protecting our nation's critical infrastructure from targeted attacks. Protecting our nation's interconnected and interdependent infrastructure also requires a robust public-private partnership that provides the private sector with information on incidents, threats, and vulnerabilities, as well as protects private sector information in such a way that the private sector is willing to share it with government partners. Thus, an effective framework that ensures a two-way flow of timely, actionable threat information between public and private partners is essential to achieving success in the war on terrorism.

As the owners and operators of the vast majority of the nation's critical infrastructure, private industry possesses information of potential value to the Federal government; and at the same time, it needs and seeks access to information from the Federal government for situational awareness, to manage risks to enterprises, and to understand the national security implications posed by terrorist threats.

Efforts to improve sharing of terrorism information with the private sector are ongoing. These activities are based on the authority provided to the Secretary of Homeland Security by the Homeland Security Act of 2002 and Homeland Security Presidential Directive 7 (HSPD-7), which defines infrastructure protection responsibilities for DHS, sector-specific agencies, and other departments and agencies. Specifically, HSPD-7 instructs Federal departments and agencies to identify, prioritize, and coordinate the protection of critical infrastructure to prevent, deter, and mitigate the effects of attacks. In addition, the National Infrastructure Protection Plan (NIPP), recently released by DHS, is the cornerstone document that prescribes a national implementation strategy for HSPD-7 and creates a public-private partnership structure and mechanisms through which to carry it out. The requirements and tasks identified in these documents require an efficient and effective two-way flow of information between Federal and State, local, and tribal officials and private sector partners.

The President also created the National Infrastructure Advisory Council (NIAC). The NIAC is charged to improve the cooperation and partnership between the public and private sectors in securing the critical infrastructures and advises the President and Secretary of Homeland Security on policies and strategies that range from risk assessment and management to information sharing, protective strategies, and clarification on roles and responsibilities between public and private sectors.

Accordingly, sharing terrorism information with the private sector requires:

- Building a trusted relationship between the Federal, State, local, and tribal officials and private partners to facilitate information sharing. In some cases, establishing such relationships may be difficult because sector-specific agencies may also have a regulatory role.

- Improving the two-way sharing of terrorism information on incidents, threats, consequences, and vulnerabilities. Most critical infrastructure sectors, like their State, local, and tribal partners, are still concerned about the limited quantity and quality of information available and the perceived need for more specific, timely, and actionable information. Likewise, Federal, State, local, and tribal officials need to have policies in place that will ensure the protection of private sector vulnerability information that is shared with government partners.

- Integrating private sector analytical efforts into Federal, State, local, and tribal processes, as appropriate, for a more complete understanding of our terrorism landscape. The private sector understands its processes, assets, and operations best and can provide the required private sector subject matter expertise.

- Establishing mechanisms and processes to ensure compliance with all relevant U.S. laws, including applicable privacy and civil liberty laws.

## VI. Findings and Recommendations

### *General Findings and Recommendations:*

**Finding 1:** In order to ensure effective and immediate implementation of this framework, a senior level interagency advisory group must be established to oversee the implementation process.

**Recommendation 1:** Within 30 days of approval of the proposed framework, a senior-level advisory group should be established to ensure accountability, oversight, and governance for the effective operation of this framework. The advisory group should be composed of ISC members or their designees and should report the results of its oversight to the ISC. The advisory group should meet at least once per month during the first year of implementation.

**Finding 2:** As it relates to the retention and use of homeland security information, terrorism information, and law enforcement information, practices must acknowledge the authority of originating organizations to approve follow-on use and/or disposition of the information, but organization-specific controls should be the exception and reflect the expectations and accountability for information sharing set by the head of the responsible agency.

**Recommendation 2:** Policies, protocols, and procedures should be clarified to allow the most effective retention and use of homeland security information, terrorism information, and law enforcement information while also respecting the need of organizations, in appropriate circumstances, to protect sensitive data, including sources

and methods of collection. NCTC's practices in this area may provide a model upon which these policies, protocols, and procedures can be developed.

**Finding 3:** There is a need to develop processes to communicate threat and risk assessments, associated requirements and tasks, and reporting responsive to those requirements and tasks, between Federal agencies and departments and State, local, and tribal entities in a bi-directional manner.

**Recommendation 3:** DOJ and DHS should establish a coordinated set of policies, protocols, and procedures to support the following:

1. Drawing upon existing and ongoing efforts at the Federal level, develop, maintain, and, as appropriate, disseminate an assessment of terrorist risks and threats;

2. Use of the risk and threat assessment to identify and gather information responsive to the identified threats and risks;

3. Define the means through which Federal data related to terrorist risks and threats and associated requirements and tasks is communicated to State, local, and tribal authorities and private sector entities;

4. Define the means through which State, local, tribal, and private sector data related to terrorist risks and threats and associated requirements and tasks is communicated to Federal authorities;

5. Develop the processes and protocols for ensuring that priority information is provided to those entities responsible for assessing national patterns and trends analysis;

6. Identify requirements for a centralized system for reporting, tracking, and accessing suspicious incidents and activities; and

7. Design a mechanism to monitor and refine the above processes.

### *Recommendations to address Federal to Federal Sharing*

**Finding 4:** A senior level interagency Implementation Team is needed to guide the establishment of the Interagency Threat Assessment Coordination Group proposed in the framework.

**Recommendation 4A:** Establish an Implementation Team within 7 days comprised of representatives from DoD, DOJ, DHS, FBI, NCTC, the PM-ISE, and appropriate State, local, and tribal entities, and including consultation with other departments and

agencies, as appropriate, for the purposes of developing an implementation plan for this framework and ensuring its timely execution. Specifically the Implementation Team will be responsible for:

1. Refining the standards and practices to govern Federal, State, local, and tribal officials and private section interaction through the network of fusion centers linked to the national coordination group;

2. Effecting the staffing and stand-up of the coordination group;

3. Ensuring compliance with applicable laws and regulations, including all U.S. laws protecting individuals' privacy and civil liberties; and

4. Engaging in a campaign to notify and educate Federal, State, local, and tribal officials and private sector entities of the existence, function, and responsibilities of the coordination group established by Guideline 2.

**Recommendation 4B:** As part of efforts to monitor the progress of ISE implementation, within 180 days of approval of this framework, Federal members of the Implementation Team, on behalf of the participating Federal entities, after seeking appropriate input from State, local, and tribal representatives, should submit to the PM-ISE an interim report identifying and discussing the successes and shortcomings experienced to date in the implementation and operation of the governing framework and outlining steps to be undertaken to refine and improve the framework's operation. Any disputes and/or issues requiring resolution will be addressed through the White House policy process.

### *Recommendations to address sharing with and among State, local, and tribal officials*

**Finding 5:** States and major urban area fusion centers should continue to maintain and/or develop the capacity to support a number of critical counterterrorism, homeland security, and homeland defense-related activities, including but not limited to the development and/or maintenance of:

1. Mechanisms to contribute information of value to ongoing Federal and national-level assessments of terrorist risks;

2. Statewide, regional, site-specific, and topical risk assessments;[1]

[1] *These assessments support DHS' critical infrastructure protection and preparedness planning efforts as well as DoD's force protection activities and provide situational awareness for the FBI's investigations and intelligence gathering activities.*

3. Processes in support of information responsive to Federally-communicated requirements and tasks;

4. Alerts, warning, notifications, advisories, and bulletins regarding time sensitive or strategic threats;

5. Situational awareness reports; and

6. Analytical reports regarding incidents or specific threats.

**Recommendation 5A:** Request that State Governors designate one fusion center with capacity sufficient to serve as the statewide center or hub to interface with the Federal government and through which to coordinate the gathering, processing, analysis, and dissemination of homeland security information, terrorism information, and law enforcement information on a statewide basis. At the same time, the executive agent of each major urban as well as the applicable State's homeland security advisor should work together to determine the most effective manner in which to incorporate the Urban Area Security Initiative (UASI) into the information sharing framework. In those instances in which the UASI has established a regional fusion center, consideration will be given to incorporating those major urban area fusion centers into the framework.

**Recommendation 5B:** Request that DOJ and DHS, to the maximum extent practicable, provide technical assistance and training to support the establishment and proper functioning of these fusion centers.

**Recommendation 5C:** Request DOJ and DHS to amend grants guidance and technical assistance to ensure that fusion center grant recipients, as a condition of receiving funding, meet delineated baseline capability requirements.

**Recommendation 5D:** Ensure that in furtherance of this shared-responsibility approach, participating Federal entities also will undertake other efforts to ensure effective implementation and operation of the framework by:

1. Wherever practical, assigning representative personnel to State and local fusion centers and otherwise striving to integrate and, to the extent practicable, collocate resources; and

2. Ensuring that all personnel working within the framework understand the framework's essential attributes and the necessity for close coordination and collaboration with Federal counterparts and State, local, and tribal partners.

**Recommendation 5E:** DOJ and DHS, in consultation with the Program Manager's Office, shall develop standards to assist State and major urban area fusion centers to achieve capacity to:

1. Develop, maintain, and, as appropriate, disseminate assessments of terrorist risks and threats gathered at the State, local, or tribal level;

2. Use risk and threat assessments to identify and gather information responsive to identified threats and risks;

3. Develop the processes and protocols for ensuring that priority information — including Suspicious Incident Reports (SIRs) and Suspicious Activity Reports (SARs) — is reported to the appropriate law enforcement authorities and national entities to support its inclusion into national patterns and trends analysis; and

4. Specify the means through which the State, local, and tribal data related to terrorist risks and threats and associated requirements and tasks is communicated to Federal authorities and private sector entities.

### *Recommendations to address sharing with the Private Sector*

**Finding 6:** A significant mechanism for sharing terrorism information from the Federal government to private sector entities is through the Sector Partnership framework described in the NIPP where DHS works with Sector Specific Agencies, Government Coordinating Councils (GCCs), Sector Coordinating Councils (SSCs), and — where designated by SCCs — sector specific Information Sharing and Analysis Centers (ISACs).

**Recommendation 6:** DHS must increase its ability to share information in a manner that protects the privacy, civil liberties, and other legal rights of individuals and corporations, as provided for under U.S. law, so that private sector entities can manage risks to their business enterprises, by:

1. Creating a national framework and culture for sharing information that rationalizes requests for terrorism information to the private sector and that adequately protects the risks and proprietary interests of corporations;

2. Identifying—and keeping current—a roster of industry operational and technical experts from across industries who can assist in preventing, detecting, deterring, and responding to terrorist threats;

3. Creating an integrated, trusted environment in which information from the private sector can be shared, maintained, and protected;

4. Ensuring that economic recovery and infrastructure protection are major aspects of responding to a terrorist incident, bolstering public confidence, and continuing to deliver critical infrastructure services;

5. Integrating the analysis of data from multiple sources to provide industry with indicators of impending threats or current attacks;

6. Coordinating with related initiatives in place with other departments and agencies;

7. Disseminating actionable alerts and warnings concerning specific private sectors that improve their situational awareness of terrorist threats and enable them to prioritize risks and security investments, and shape the development of plans to ensure the security, continuity, and resiliency of infrastructure operations; and

8. Implementing policies and mechanisms that provide liability and antitrust protections to the private sector for sharing information in good faith.