Attached for your review is the working draft National Prevention Framework.

This framework is meant to address a number of key issues related to Prevention, including:

- Describe the roles and responsibilities of all stakeholders.
- Define the coordinating structures—either new or existing—that enable the effective delivery of the core capabilities.
- Convey how actions are integrated with other mission areas and across the whole community.
- Identify relevant planning assumptions required to inform the development of interagency operational plans and department level plans.
- Provide information that state, territorial, tribal, and local governments and private sector partners can use to develop or revise their plans.

The enclosed working draft represents input and ideas from a range of stakeholders within and outside the Federal Government who have been involved through working groups, outreach sessions, and targeted engagement efforts in order to develop this working draft. It also draws from lessons learned over the last decade of large-scale and catastrophic events.

With all of this work in mind, it is time to further expand the engagement of the whole community in the development of this framework. We are therefore seeking your ideas and input on this working draft.

To ensure all feedback is properly handled, reviewers are expected to use the feedback submission form to submit your feedback. All feedback should be submitted, using the submission form, to PPD8-Engagement@fema.gov by the following deadline: **Monday, April 2, 2012 at 12:00 PM EDT**. Please include the word “**Prevention**” in the subject line.

We look forward to receiving your feedback and working in partnership with you on this important endeavor.

For further information on the PPD-8 effort, visit [http://www.fema.gov/ppd8](http://www.fema.gov/ppd8) or send an e-mail to PPD8-Engagement@fema.gov.
A terrorist threat is considered *imminent* if intelligence or operational information warns of a credible, specific, and impending terrorist threat or ongoing attack against the United States that is sufficiently specific and credible to recommend implementation of additional measures to thwart an attack.

1 The National Preparedness Goal is located at http://www.fema.gov/ppd8.
Terrorism prevention should be conducted as far from its intended target as possible. Ideally, terrorism is addressed at its root, by countering radicalization toward a violent extremist ideology. Therefore, it is preferable to deter terrorist plots, to thwart or counter emerging terrorist plots at the earliest stages, and, if other efforts fail, to detect, disrupt, and interdict ongoing terrorist activity as far from the intended target as possible.\(^2\)

PPD-8 states that “for the purposes of the prevention framework called for in this directive, the term ‘prevention’ refers to preventing imminent threats.” Thus, the Framework applies only to those capabilities, plans, and operations necessary to ensure we are optimally prepared to prevent an imminent act of terrorism on U.S. soil, and does not capture the full spectrum of the Nation’s efforts to counterterrorism.

The National Prevention Framework recognizes that there are a host of support activities executed on an ongoing basis which support and enable terrorism prevention efforts. These support activities position all levels of government and public safety agencies to be optimally prepared to execute the core capabilities necessary to prevent an imminent terrorist threat. Specifically, the ability to quickly collect, analyze, and further disseminate intelligence becomes critical in an imminent threat situation. In order to accomplish this, law enforcement, intelligence and homeland security professionals must form engaged partnerships across the whole community.\(^3\) These partnerships are force multipliers and allow for the seamless acquisition and passage of information. The support activities include those programs, initiatives, and information sharing efforts that directly support local efforts to understand, recognize, and prevent operational activity and other crimes that are precursors or indicators of terrorist activity. In addition to Joint Terrorism Task Forces (JTTFs), Field Intelligence Groups (FIGs), and fusion centers, a variety of analytical and investigative efforts support the ability to identify and counter terrorist threats by executing these support activities. These efforts include other Federal, state, and local law enforcement agencies, and various intelligence centers and related efforts such as High Intensity Drug Trafficking Areas (HIDTA), Regional Information Sharing Systems (RISS) Centers, criminal intelligence units, real-time crime analysis centers, and others.

The National Prevention Framework focuses on how the whole community will marshal these capabilities in a rapid, coordinated approach in three potential situations:

- To stop a particular credible, specific, and impending terrorist threat.
- To prevent a follow-on terrorist attack.
- At the direction of the President.

**RISK BASIS**

The Secretary of Homeland Security led an interagency effort to conduct a Strategic National Risk Assessment (SNRA). The SNRA identifies the threats and hazards that pose the

---

\(^2\) For additional information about these activities, see the *National Strategy for Counterterrorism* (June 2011), located at http://www.whitehouse.gov/sites/default/files/counterterrorism_strategy.pdf.

\(^3\) These partnerships should support the development, implementation, and/or expansion of programs designed to partner with local communities to counter violent extremism in accordance with the *Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States* (December 2011), located at http://www.whitehouse.gov/sites/default/files/sip-final.pdf.
greatest risk to the Nation. In turn, the National Preparedness Goal identifies the core capabilities essential to address these risks in each of the five preparedness mission areas. This Framework addresses delivery of the core capabilities required to address the following adversarial/human-caused risks.

**Exhibit 1: SNRA Adversarial/Human-Caused National-level Events**

<table>
<thead>
<tr>
<th>Row</th>
<th>Threat Type</th>
<th>National-level Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Aircraft as a Weapon</td>
<td>A hostile non-State actor(s) crashes a commercial or general aviation aircraft into a physical target within the United States</td>
</tr>
<tr>
<td>2</td>
<td>Armed Assault</td>
<td>A hostile non-State actor(s) uses assault tactics to conduct strikes on vulnerable target(s) within the United States resulting in at least one fatality or injury</td>
</tr>
<tr>
<td>3</td>
<td>Biological Terrorism Attack (non-food)</td>
<td>A hostile non-State actor(s) releases a biological agent against an outdoor, indoor, or water target, directed at a concentration of people within the United States</td>
</tr>
<tr>
<td>4</td>
<td>Chemical/Biological Food Contamination Terrorism Attack</td>
<td>A hostile non-State actor(s) disperses a biological or chemical agent into food supplies within the U.S. supply chain</td>
</tr>
<tr>
<td>5</td>
<td>Chemical Terrorism Attack (non-food)</td>
<td>A hostile non-State actor(s) releases a chemical agent against an outdoor, indoor, or water target, directed at a concentration of people using an aerosol, ingestion, or dermal route of exposure</td>
</tr>
<tr>
<td>6</td>
<td>Explosives Terrorism Attack</td>
<td>A hostile non-State actor(s) deploys a man-portable improvised explosive device (IED), vehicle-borne IED, or vessel IED in the United States against a concentration of people, and/or structures such as critical commercial or government facilities, transportation targets, or critical infrastructure sites, etc., resulting in at least one fatality or injury</td>
</tr>
<tr>
<td>7</td>
<td>Nuclear Terrorism Attack</td>
<td>A hostile non-State actor(s) acquires an improvised nuclear weapon through manufacture from fissile material, purchase, or theft and detonates it within a major U.S. population center</td>
</tr>
<tr>
<td>8</td>
<td>Radiological Terrorism Attack</td>
<td>A hostile non-State actor(s) acquires radiological materials and disperses them through explosive or other means (e.g., a radiological dispersal device [RDD]) or creates a radiation exposure device (RED)</td>
</tr>
</tbody>
</table>

The Framework focuses on the development and execution of core capabilities to maximize the Nation’s preparedness to prevent these adversarial/human-caused incidents. These threats may manifest as conventional or as weapons of mass destruction (WMD) attacks; as multiple, geographically dispersed, near-simultaneous attacks; or as a coordinated campaign over a prolonged period of time.

The Prevention mission area is focused exclusively on terrorist threats; the other four preparedness mission areas are “all hazards.” In addition to the terrorist threats identified above, the SNRA identifies a range of hazards (natural disasters, pandemics, technological accidents, and cyber attacks) that pose a risk to the safety and security of our Nation. These hazards, and the core capabilities required to address them, are addressed in the other four preparedness mission areas, as appropriate.
All levels of government, private and non-profit sector organizations, communities, and households should assess their particular risks to identify capability requirements and prioritize their preparedness efforts.

**INTENDED AUDIENCE**

The Framework can be helpful to every U.S. citizen and resident, but is intended to be especially useful for government leaders and practitioners who have a responsibility to prevent terrorist attacks on the homeland. Senior leaders, such as Federal department or agency heads, State Governors, mayors, tribal leaders, police chiefs, commissioners, sheriffs, and other city or county officials should use the Framework as a comprehensive and accessible reference guide to the core capabilities needed to prevent imminent acts of terrorism. In a resource constrained environment, the Framework provides senior decision makers with an understanding of where existing investments must be sustained and where new investments must be made in order to ensure our Nation is optimally prepared to prevent an imminent terrorist attack.

The Framework also provides guidance to intelligence and law enforcement professionals on how existing structures; such as the Federal Bureau of Investigation’s (FBI’s) JTTFs, state and major urban area fusion centers, and state and local counterterrorism and intelligence units; can collaborate and prioritize their efforts to support the delivery of Prevention core capabilities. Finally, the Framework is also for communities and citizens. It outlines the role of the public in terrorism prevention, especially in reporting potentially terrorism related or suspicious activities. The Framework explains how the general public and private sector may serve as a force multiplier for law enforcement in terrorism prevention.

**GUIDING PRINCIPLES FOR PREVENTION**

The desired end state of Prevention is a Nation optimally prepared to prevent an imminent terrorist attack within the United States. To achieve this end state, the Framework sets out three principles that guide development and execution of the core capabilities for Prevention: (1) engaged partnership; (2) scalability, flexibility, and adaptability; and (3) readiness to act.

1. **Engaged Partnership.** The prevention of terrorism is a shared responsibility among the various Federal, state, local, and non-profit and private sector entities that comprise the whole community. Each level of government must play a prominent role in building capabilities, developing plans, and conducting exercises to prepare to prevent an imminent terrorist attack. In addition, individuals, non-profit and private sector entities, and international partners can all provide critical assistance.

2. **Core capabilities are scalable, flexible, and adaptable and executed as needed to address the full range of threats as they evolve.** Depending on the nature, scope, or location of the threat, officials from all levels of government may elect to execute some or all core capabilities covered in this Framework. The coordinating structures outlined in the Framework can be tailored and leveraged to marshal the appropriate core capabilities to defeat the threat.

---

4 For the purposes of this document, “state and local” includes tribal and territorial governments.
(3) The whole community builds and maintains the core capabilities in order to execute them either before an attack, based on knowledge of an imminent threat or after an incident to prevent follow-on attacks and/or apprehend the adversary (i.e., readiness to act).

RELATIONSHIP TO OTHER MISSION AREAS

PPD-8 mandates the National Prevention Framework as one of a series of integrated national planning frameworks in the National Planning System. The National Planning System is an essential part of the National Preparedness System, which guides, organizes, and unifies our Nation’s homeland security efforts to support achievement of the National Preparedness Goal.

Recognizing that Prevention efforts may occur simultaneously with other efforts, especially Protection and Response, the core capabilities and coordinating structures of the Framework can be integrated with those established in the other national planning frameworks. This interoperability is integral to achieving the National Preparedness Goal.

- Protection. Prevention and Protection are closely aligned. The Prevention mission area focuses on those intelligence, law enforcement, and homeland security activities which prevent an adversary from carrying out an attack within the United States. Protection activities focus on decreasing the likelihood of an attack within the homeland. Protection and Prevention share a number of common elements and rely on many of the same core capabilities. Protection and Prevention processes described in these frameworks are designed to operate simultaneously and to complimentary with each other.

- Mitigation. The law enforcement, intelligence, and homeland security communities play a significant role in Mitigation. Outreach and community involvement help to establish and maintain strong ties with neighbors, businesses, academic institutions, and critical infrastructure owners and operators. Intelligence-focused relationships among Federal, state, and local law enforcement, intelligence and homeland security entities, and with the public and private sector, academia, and other community organizations facilitate information sharing. In turn, this creates more opportunities to thwart acts of terrorism and to lessen the effects of large-scale, man-made catastrophes should they occur. Through these dialogues, communities may better detect and deter specific threats and mitigate vulnerabilities. They may also develop new ways of reducing risks and reporting successful practices. Finally, through integrated and risk-informed planning efforts, law enforcement and homeland security partners can help improve the whole community’s ability to avoid future loss of life and property.
### Exhibit 2: Core Capabilities by Preparedness Mission Area

<table>
<thead>
<tr>
<th>Row</th>
<th>Prevention</th>
<th>Protection</th>
<th>Mitigation</th>
<th>Response</th>
<th>Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Planning</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Public Information and Warning</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Operational Coordination</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Intelligence and Information Sharing</td>
<td>Intelligence and Information Sharing</td>
<td>Community Resilience</td>
<td>Critical Transportation</td>
<td>Economic Recovery</td>
</tr>
<tr>
<td>5</td>
<td>Screening, Search and Detection</td>
<td>Screening, Search and Detection</td>
<td>Long-term Vulnerability Reduction</td>
<td>Environmental Response/Health and Safety</td>
<td>Health and Social Resources</td>
</tr>
<tr>
<td>6</td>
<td>Interdiction and Disruption</td>
<td>Interdiction and Disruption</td>
<td>Risk and Disaster Resilience Assessment</td>
<td>Fatality Management Services</td>
<td>Natural and Cultural Resources</td>
</tr>
<tr>
<td>7</td>
<td>Forensics and Attribution</td>
<td>Access Control and Identity Verification</td>
<td>Threat and Hazard Identification</td>
<td>Infrastructure Systems</td>
<td>Infrastructure Systems</td>
</tr>
<tr>
<td>8</td>
<td>Cybersecurity</td>
<td></td>
<td></td>
<td>Mass Care Services</td>
<td>Housing</td>
</tr>
<tr>
<td>9</td>
<td>Physical Protective Measures</td>
<td></td>
<td></td>
<td>Mass Search and Rescue Operations</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Risk Management for Protection Programs and Activities</td>
<td></td>
<td></td>
<td>Public Health and Medical Services</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Supply Chain Integrity and Security</td>
<td></td>
<td></td>
<td>On-Scene Security and Protection</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td>Public and Private Services and Resources</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td></td>
<td></td>
<td></td>
<td>Operational Communications</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td></td>
<td></td>
<td></td>
<td>Situational Assessment</td>
<td></td>
</tr>
</tbody>
</table>

**Response and Recovery.** As with the other mission areas, Prevention and Response share three core capabilities. In addition, Prevention involves processing the scene of a terror attack for forensic evidence while Response will likely be working at the same time in the same space to save lives and minimize loss. This requires synchronization through the operational coordination of efforts, likely to occur in a Joint Operations Center in conjunction with the Joint Field Office. Similarly, Prevention and Response related authorities must be in communication during times...
of an imminent threat so that Response assets, to the extent practical and appropriate, may be pre-positioned. Both Response and Recovery functions personnel will be unable to access the scene of a terrorist attack until criminal investigators and forensics teams finish their work. But, Prevention assets will provide Response and Recovery personnel data concerning contamination in the impacted area which will assist response and recovery activities. In many cases, Prevention will be working simultaneously with Recovery in this regard.

The Nation relies on these shared core capabilities prior to or in the absence of an imminent threat situation. Perhaps most importantly, this Framework recognizes that upon an imminent threat, having already established the ability to quickly collect, analyze, and further disseminate intelligence becomes critical. To do this successfully, relationships must already be developed, access points of where information can be collected must already be identified, analysts must already be adequately trained and have access to appropriate classified and unclassified systems/databases, and the communities that are best positioned to recognize the steps just prior to an attack must already be prepared to do so. These pre-imminent support activities position all levels of government and public safety agencies to effectively prevent an imminent threat once it is identified.

Section 4.0 of this Framework describes how each core capability listed above is utilized in the prevention of an imminent terrorist attack on the homeland.

3.0 ROLES AND RESPONSIBILITIES

This section provides an overview of who has a role to play in implementing the National Prevention Framework. Federal, state, and local partners have roles and responsibilities for Prevention. Prevention also includes an important role for community members and the private sector. Together we must prepare and deliver essential core capabilities to prevent terrorist attacks on the United States.

Individuals and households can play an important role in the prevention of terrorism by identifying and submitting potential terrorism-related information and/or suspicious activity reports to law enforcement. Individual vigilance and awareness can help communities remain safer and bolster prevention efforts.

Communities and community organizations foster the development of organizations and organizational capacity that act toward a common goal (such as a local neighborhood watch). These groups may possess the knowledge and understanding of the threats within their jurisdictions and have the capacity necessary to alert authorities of those threats, capabilities, or needs by identifying and submitting potential terrorism-related information and/or suspicious activity reports to law enforcement.

Private and non-profit sector entities operate in all sectors of trade and commerce that foster the American way of life and support the operation, security, and resilience of global movement systems. Private and non-profit sector entities can assist in the prevention of terrorism by identifying and submitting potential terrorism-related information and/or suspicious activity reports to law enforcement.

Local governments provide front-line leadership for local law enforcement, fire, public safety, environmental response, public health, and emergency medical services for all manner of threats, hazards and emergencies. Local governments coordinate resources and capabilities
Local law enforcement agencies are responsible for the preservation of peace, the protection of life and property, the prevention of crime, and the arrest of violators of the law. These agencies engage in community and interagency partnerships so as to identify and prevent criminal acts to include terrorism and transnational threats.

State and territorial governments coordinate activity in support of cities, counties, and intrastate regions. State agencies conduct law enforcement, intelligence, and security activities. During an incident, states coordinate resources and capabilities throughout the state and often mobilize these resources and capabilities to supplement local efforts should an incident occur. States also administer Federal homeland security grants to local and tribal (in certain grant programs) governments, allocating key resources to bolster their prevention and preparedness capabilities. Governors are responsible for overseeing their state’s threat prevention activities as well as the state’s response to any emergency. Should and incident occur, governors will play a number of roles, including the state’s chief communicator and primary source of information on an incident. Governors are commanders of their National Guards and are able to call them up to assist under state active duty, and also retain command over their National Guard under Title 32 status. During an incident, governors will also make decisions regarding requests for mutual aid and calls for Federal assistance.

Tribal governments engage in a government-to-government relationship with the Federal Government and have special status under Federal laws and treaties. Tribal governments provide essential services to members and non-members residing within their jurisdictional boundaries. Depending on the availability of resources and complex jurisdictional issues, tribal governments may provide law enforcement services for their members in addition to fire and emergency services throughout their jurisdictions. Tribal leaders are responsible for overseeing the tribe’s engagement with Federal, state, and local programs.

The Federal Government carries out statutory and regulatory responsibilities for a wide array of Prevention programs and provides assistance in a number of areas, including funding, research, coordination, oversight and implementation.

The President of the United States leads the Federal Government’s effort to ensure that the necessary coordinating structures, leadership, and resources are applied effectively and efficiently to prevent an imminent terrorist attack from occurring. The President receives advice from Cabinet officials and other department or agency heads as necessary to make decisions about Federal activities prior to an imminent terrorist attack.

The Department of Justice, under the Attorney General, has lead responsibility for criminal investigations of terrorist acts or terrorist threats by individuals or groups inside the United States, or directed at U.S. citizens or institutions abroad, as well as for related intelligence collection activities within the United States, subject to the National Security Act of 1947, other applicable law, Executive Order 12333, and Attorney General-approved procedures pursuant to that Executive Order. Generally acting through the Federal Bureau of Investigation, the Attorney General, in cooperation with other Federal departments and agencies engaged in activities to protect national security, shall also coordinate the activities of the other members of the law enforcement community to detect, prevent, preempt, and disrupt terrorist attacks against the United States.
The Secretary of Homeland Security leads the Federal interagency in securing the homeland against terrorism and other threats and hazards. The role of the Department of Homeland Security (DHS) in preventing terrorism includes assessing and managing terrorism risk; preventing terrorists from entering or remaining in the country; preventing acquisition of WMD-related materials and/or weapons; preventing importation of weapons and weapons-related materials through screening, search, detection, and interdiction; preventing the use of our transportation systems for terrorististic purposes; and interdicting terrorist activity within the maritime, air, and land domains. DHS coordinates its actions with the interagency, and when appropriate, coordinates interagency actions. Finally, DHS shares information on terrorist threats with Federal, state, and local governments and private sector partners.

The Director of National Intelligence (DNI) serves as the head of the Intelligence Community (IC), acts as the principal advisor to the President and National Security Council for intelligence matters relating to national security, and oversees and directs implementation of the National Intelligence Program. The IC, composed of 16 elements across the Federal Government, functions consistent with law, Executive Order, regulations, and policy to support the national security-related missions of the U.S. Government. It provides a range of analytic products that assess threats to the homeland and inform planning, capability development, and operational activities of homeland security enterprise partners and stakeholders. In addition to IC elements with specific homeland security missions, the Office of the Director of National Intelligence maintains a number of mission and support centers that provide unique capabilities for homeland security partners, including the National Counterterrorism Center (NCTC), National Counterproliferation Center, and National Counterintelligence Executive. NCTC serves as the primary U.S. Government organization for analyzing and integrating all intelligence pertaining to terrorism and counterterrorism, and conducts strategic operational planning for integrated counterterrorism activities.

The Department of Defense (DoD) conducts homeland defense and civil support missions to prevent an imminent terrorist attack from occurring. DoD leads the homeland defense mission to protect U.S. sovereignty, U.S. territory, the domestic population, and the defense industrial base against external threats and aggression or other threats as directed by the President. DoD also provides defense support to civil authorities for domestic incidents as directed by the President or when consistent with military readiness and appropriate under the circumstances and the law (HSPD-5). At the request of the Secretary of Homeland Security, DoD support may include, but is not limited to, monitoring and interdicting WMD materials at borders, ports of entry, and other locations within the U.S. At the request of the Attorney General, DoD support to law enforcement may include, but is not limited to, incident awareness and assessment, search and detection, interdiction and disruption, forensics and attribution, planning, and transportation and logistics support.

The Department of State conducts the diplomacy and foreign policy of the United States and employs its authorities and resources pertaining to international prevention of terrorist activities. The Department of State works closely with international partner nations and regional and multilateral organizations in these terrorism prevention efforts to address foreign threats against the U.S. homeland.

In accordance with the President’s intent as outlined in the National Security Strategy, preventing a terrorist attack requires a whole of government approach. To that end, under the National Prevention Framework, and consistent with existing law, Executive Orders, regulations
and policy, various other Federal departments and agencies may play primary, coordinating
and/or supporting roles in the prevention of an imminent act of terrorism based on their
authorities and resources and the nature of the threat or incident. While not called out
individually, many Federal agencies and departments contribute greatly to the prevention effort.

4.0 CORE CAPABILITIES

Building on the National Preparedness Goal, this chapter provides a robust explanation of
what each Prevention core capability entails and the context in which the Nation must be
prepared to execute it. This is not intended to be an exhaustive list of all capabilities and critical
tasks that may be required to prevent an imminent terrorist threat. Rather, it is a description of
the capabilities and tasks the whole community will most likely need to achieve the desired end
state of a Nation that is optimally prepared to prevent an imminent terrorist attack on the
homeland.

INTELLIGENCE AND INFORMATION SHARING

Description: To identify, develop, and provide timely, accurate, and actionable
information resulting from the planning, direction, collection, exploitation, processing, analysis,
production, dissemination, evaluation, and feedback of available information concerning
imminent terrorist threats to the United States, its people, property, or interests; the development,
proliferation, or use of WMD; or any other matter bearing on U.S. national or homeland security
by Federal, state, and local governments and other stakeholders. Information sharing is the
ability to exchange intelligence, information, data, or knowledge among Federal, state, and local
governments, private sector entities, or international partners as appropriate.

<table>
<thead>
<tr>
<th>Row</th>
<th>Target Objectives for Intelligence and Information Sharing</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Anticipate and identify emerging and/or imminent threats through the intelligence cycle.</td>
</tr>
<tr>
<td>2</td>
<td>Share relevant, timely, and actionable information and analysis with Federal, state, local, private sector, and international partners and develop and disseminate appropriate classified/unclassified products.</td>
</tr>
<tr>
<td>3</td>
<td>Ensure Federal, state, local, and private sector partners possess or have access to a mechanism to submit terrorism-related information and/or suspicious activity reports to law enforcement.</td>
</tr>
</tbody>
</table>

In the context of Prevention, the Intelligence and Information Sharing capability involves
the effective implementation of the intelligence cycle and information fusion process by Federal,
state, and local intelligence entities, the private sector, and the public to develop situational
awareness on the actor(s), method(s), or weapon(s) related to an imminent terrorist threat within
the United States.

Events over the last decade have demonstrated that the ability to responsibly share
information is a prerequisite for preventing terrorist threats to our homeland. No single agency,
department, or level of government has a complete threat picture of all emergent terrorism and
national security threats. With this in mind, the Intelligence and Information Sharing capability
involves engagement across Federal, state, local, and private sector partners to: facilitate
collection, analysis, and sharing of suspicious activity reports to further support the identification
and prevention of terrorist threats; enhance situational awareness of threats, alerts, and warnings;
and develop and disseminate risk assessments and analysis of national intelligence to state, local, and private sector partners.

This capability relies on the analytical and information sharing capabilities of JTTFs and state and major urban area fusion centers during times of imminent threat, in accordance with existing laws, directives, and policies. It involves reprioritization and retasking of law enforcement and intelligence assets as necessary and appropriate. Amplifying information will also be obtained via law enforcement operations.

Together, these efforts inform local policing and enable partners at all levels of government, the private sector, and citizens to implement the most effective protective and preventive measures.

Finally, the Intelligence and Information Sharing capability recognizes that efforts to identify and counter terrorist threats will require ongoing coordination between the aforementioned efforts and other analytic and investigative efforts.

**Critical Tasks**

- **Planning and Direction:** Establish the intelligence and information requirements of the consumer.
  - Rapidly reprioritize law enforcement and intelligence assets, as necessary and appropriate.
  - Engage with private sector partners in order to determine what intelligence and information assets may be available for reprioritization.
  - Request additional intelligence requirements via law enforcement deployment, questioning of witnesses and suspects, increased surveillance activity, community policing and outreach, etc.

- **Collection:** Gather the required raw data to produce the desired finished intelligence and information products.
  - Gather/collect information via law enforcement operations, suspicious activity reporting, surveillance, community engagement, and other activities and sources as necessary.

- **Exploitation and Processing:** Convert raw data into comprehensible forms that can be utilized to produce finished intelligence and information products.

- **Analysis and Production:** Integrate, evaluate, analyze, and prepare the processed information for inclusion in the finished product.

- **Dissemination:** Deliver finished intelligence and information products to the consumer and others as applicable.

---

5 Fusion center capabilities and operations should be executed in a manner consistent with the Baseline Capabilities for State and Major Urban Area Fusion Centers (September 2008), which is located at http://it.ojp.gov/documents/baselinecapabilitiesa.pdf.
When necessary, develop appropriately classified/unclassified products to disseminate threat information to Federal, state, local, international, private and nonprofit sector, and public partners.

- Adhere to mechanisms for safeguarding sensitive information, consistent with Executive Order 13587.6

Evaluation and Feedback: Acquire continual feedback during the intelligence cycle that aids in refining each individual stage and the cycle as a whole.

Continually assess threat information to inform continued prevention operations.

**SCREENING, SEARCH, AND DETECTION**

*Description:* Identify, discover, or locate imminent terrorist threats through active and passive surveillance and search procedures. This may include the use of systematic examinations and assessments, sensor technologies, or physical investigation and intelligence.

**Exhibit 4: Target Objectives for Screening, Search and Detection**

<table>
<thead>
<tr>
<th>Row</th>
<th>Target Objectives for Screening, Search and Detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Maximize the screening of targeted cargo, conveyances, mail, baggage, and people associated with an imminent terrorist threat or act using technical, non-technical, intrusive, or non-intrusive means.</td>
</tr>
<tr>
<td>2</td>
<td>Initiate operations immediately to locate persons and networks associated with an imminent terrorist threat or act.</td>
</tr>
<tr>
<td>3</td>
<td>Conduct chemical, biological, radiological, nuclear, and explosive (CBRNE) search/detection operations in multiple locations and in all environments, consistent with established protocols.</td>
</tr>
</tbody>
</table>

In the context of Prevention, this capability includes the measures taken over-and-above routine screening and detection activities to locate specific threats. These measures may be taken in response to actionable intelligence that indicates potential targets, approach vectors, or type of weapon to be used. They may also be taken to verify or characterize the threat of materials or weapons that have already been located. Search and detection operations may be conducted with limited or no intelligence about the location of the threat, which would require the Nation to prioritize its search and detection resources.

This capability includes action taken to detect terrorist attacks in the planning, progress, or execution phases. The whole community potentially has a role to play in this capability, whether as an observant member of the public, the owner of critical infrastructure, or a law enforcement agency. The fully developed capability means the whole community is optimally prepared to quickly and effectively identify and locate terrorists and their means and methods of terrorism to prevent an imminent terrorist act within the United States.

**Critical Tasks**

- Locate persons and networks associated with an imminent terrorist threat.

---

6 Executive Order 13587 directs structural reforms aimed at strengthening oversight regarding the responsible sharing and safeguarding of classified information access and use.
• Develop and engage an observant Nation (individuals; families; communities; state, and local partners; and industry).

• Screen persons, baggage, mail, cargo and conveyances using technical, non-technical, intrusive, and non-intrusive means.
  o Consider additional measures for high risk persons, conveyances, or items.

• Conduct physical searches.

• Conduct CBRNE search/detection operations.
  o Conduct ambient and active detection of CBRNE agents.
  o Operate in a hazardous environment.
  o Conduct technical search/detection operations.
  o Conduct non-technical search/detection operations.
  o Consider deployment of Federal teams and capabilities to enhance state and local efforts including use of incident assessment and awareness assets.

• Conduct medical surveillance.

• Employ wide-area search and detection assets in targeted region in concert with state and local personnel or other Federal agencies (depending on threat).

We must always seek to improve our ability to search for and detect the full range of terrorist threats. It is especially important to conduct CBRNE screening, search, and detection operations to prevent the most catastrophic incidents.

INTERDICTION AND DISRUPTION

Description: Delay, divert, intercept, halt, apprehend, or secure imminent threats.

Exhibit 5: Target Objectives for Interdiction and Disruption

<table>
<thead>
<tr>
<th>Row</th>
<th>Target Objectives for Interdiction and Disruption</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Maximize our ability to interdict specific conveyances, cargo, and persons associated with an imminent terrorist threat or act in the land, air, and maritime domains to prevent entry into the United States or to prevent an incident from occurring in the Nation.</td>
</tr>
<tr>
<td>2</td>
<td>Conduct operations to render safe and dispose of CBRNE hazards in multiple locations and in all environments, consistent with established protocols.</td>
</tr>
<tr>
<td>3</td>
<td>Prevent terrorism financial/material support from reaching its target, consistent with established protocols.</td>
</tr>
<tr>
<td>4</td>
<td>Prevent terrorist acquisition of and the transfer of CBRNE materials, precursors, and related technology, consistent with established protocols.</td>
</tr>
<tr>
<td>5</td>
<td>Conduct tactical counterterrorism operations in multiple locations and in all environments, consistent with established protocols.</td>
</tr>
</tbody>
</table>

In the context of Prevention, this capability includes those interdiction and disruption activities undertaken in response to specific, actionable intelligence that indicates the location of a suspected weapon and/or perpetrator. It might also include in-extremis activities required when
a CBRNE device is encountered unexpectedly. Interdiction and disruption capabilities help to neutralize terrorist cells, operatives, and operations.

**Critical Tasks**

- Interdict conveyances, cargo, and persons associated with an imminent terrorist threat or act.
- Prevent terrorist entry into the United States and its territories.
- Prevent movement and operation of terrorists within the United States.
- Disrupt terrorist travel.
- Defeat (including Render Safe) CBRNE threats.
- Disrupt terrorist financing or prevent other material support from reaching its target.
- Conduct counter-acquisition activities to prevent terrorist acquisition and transfer of CBRNE materials, precursors, and related technology.
- Conduct tactical counterterrorism operations, potentially in multiple locations and in all environments.
- Enhance visible presence of law enforcement to deter or disrupt threat from reaching potential target(s).

We must continue to develop our capabilities to conduct tactical counterterrorism operations and to defeat CBRNE threats.

**FORENSICS AND ATTRIBUTION**

Description: Conduct forensic analysis and attribute terrorist acts (including the means and methods of terrorism) to their source(s), to include forensic analysis as well as attribution for an attack and for the preparation for an attack in an effort to prevent initial or follow-on acts and/or swiftly develop options.

**Exhibit 6: Target Objectives for Forensics and Attribution**

<table>
<thead>
<tr>
<th>Row</th>
<th>Target Objectives for Forensics and Attribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Prioritize physical evidence collection and analysis to assist in preventing initial or follow-on terrorist acts.</td>
</tr>
<tr>
<td>2</td>
<td>Prioritize CBRNE material (bulk and trace) collection and analysis to assist in preventing initial or follow-on terrorist acts.</td>
</tr>
<tr>
<td>3</td>
<td>Prioritize biometric collection and analysis to assist in preventing initial or follow-on terrorist acts.</td>
</tr>
<tr>
<td>4</td>
<td>Prioritize digital media and network exploitation to assist in preventing initial or follow-on terrorist acts.</td>
</tr>
</tbody>
</table>

Forensic examinations are critical to the process of attributing actions to individuals or entities. Attribution involves the fusion of all-source intelligence and information, including forensic evidence, into a confident conclusion about who is responsible for a pending threat or successful attack. The attribution process may differ depending on the type of attack. The United States must be able to identify the source of any type of attack, especially those types identified
In the context of Prevention, this capability may need to be delivered in a time-constrained or crisis environment. Execution of this capability would likely begin upon discovery of trace evidence at locations where suspected weapons or perpetrators may have been located, upon discovery of additional information on the current location of the threat, or upon an adversary’s claim of responsibility for an act of terrorism.

**Critical Tasks**

- Conduct physical evidence analysis.
  - Process fingerprints.
  - Conduct toxicology.
  - Conduct materials analysis (e.g., paints, tapes, inks, glass, paper, and metals).
- Conduct chemical, biological, radiological, and nuclear (CBRN) material analysis.
  - Conduct trace organic and inorganic chemical analysis.
  - Conduct microbial forensics.
- Conduct biometric analysis.
- Conduct digital media and network exploitation.
- Conduct DNA analysis.
- Identify explosives.
- Assess capabilities of likely perpetrator(s).
- Deploy investigators and technical attribution assets to identify the attack perpetrator(s).
- Interview witnesses, potential associates, and/or perpetrators if possible.
- Examine intelligence and forensics to refine/confirm attribution leads.
  - Gather samples in specific geographies or target locations.
  - Interpret and communicate attribution results and their significance to national decision makers.
- Develop databases.

**PUBLIC INFORMATION AND WARNING**

Description: Deliver coordinated, prompt, reliable, and actionable terrorism-related information to the whole community through the use of clear, consistent, accessible, and culturally and linguistically appropriate methods to effectively relay information regarding any imminent threat and, as appropriate, the actions being taken and the assistance being made available.
## Exhibit 7: Target Objectives for Public Information and Warning

<table>
<thead>
<tr>
<th>Row</th>
<th>Target Objectives for Public Information and Warning</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Share prompt and actionable messages, to include National Terrorism Advisory System (NTAS) alerts, with the public and other stakeholders, as appropriate, to aid in the prevention of imminent or follow-on terrorist attacks, consistent with the timelines specified by existing processes and protocols.</td>
</tr>
<tr>
<td>2</td>
<td>Provide public awareness information to inform the general public on how to identify and provide terrorism-related information to the appropriate law enforcement authorities, thereby enabling the public to act as a force multiplier in the prevention of imminent or follow-on acts of terrorism.</td>
</tr>
</tbody>
</table>

In the context of Prevention, this is the capability to provide the public with advanced notice regarding the potential for a terrorist attack. The process of deciding how to communicate terrorism-related information to the public must be timely and well-coordinated through standardized procedures. These procedures will inform stakeholders of pending threats, as appropriate, and provide instruction on how to take necessary precautions to protect themselves, their families, and their property. Since certain communities respond better to different types of media outreach, the decision of how to communicate with the public should be tailored to best meet the specific needs of the audience.

DHS leads the evaluation of terrorism vulnerabilities and coordinates with other Federal, state, local, and private entities to ensure the most effective response. The collection, protection, evaluation and dissemination of critical threat information to the American public, state and local governments, and the private sector is central to this task. This information is provided to the public, primarily through NTAS alerts. The NTAS system is designed to effectively communicate information about terrorist threats by providing timely, detailed information to the public, government agencies, first responders, airports and other transportation hubs, and the private sector. Depending on the nature of the threat, alerts may be sent to law enforcement, distributed to affected areas of the private sector, or issued more broadly to the public through both official and social media channels. Alerts may be broad, local, or sector specific. State and local governments may also choose to issue notices and alerts to their constituencies concerning a potential threat of terrorism, in coordination with JTTFs and fusion centers.

---

7 Under NTAS, DHS will coordinate with other Federal entities to include the FBI in order to issue detailed alerts to the public when the Federal Government receives information about a credible terrorist threat. NTAS alerts provide a concise summary of the potential threat including geographic region, mode of transportation, or critical infrastructure potentially affected by the threat, actions being taken to ensure public safety, as well as recommended steps that individuals, communities, business, and governments can take to help prevent, mitigate, or respond to a threat. NTAS alerts will also be displayed in places such as transit hubs, airports, and government buildings. These threat alerts will be issued for a specific time period and will automatically expire. Alerts may be extended if new information becomes available or as a specific threat evolves.

NTAS alerts will include a clear statement on the nature of the threat, which will be defined in one of two ways:

- **Elevated Threat:** Warns of a credible terrorist threat against the United States
- **Imminent Threat:** Warns of a credible, specific, and impending terrorist threat against the United States

Depending on the nature of the threat, alerts may be sent to law enforcement, distributed to affected areas of the private sector, or issued more broadly to the public through both official and social media channels—including a designated DHS Web site. NTAS alerts will also be displayed in places such as transit hubs, airports, and government buildings. These threat alerts will be issued for a specific time period and will automatically expire. Alerts may be extended if new information becomes available or as a specific threat evolves.
Should an NTAS alert be issued, fusion centers may be leveraged to disseminate time-sensitive NTAS alerts and associated preventive and protective measure information to fusion center partners and generate value-added analysis, information and intelligence within a local context.

**Critical Tasks**

- Increase public awareness of indicators of terrorism and terrorism-related crime, leveraging the “If You See Something, Say Something”™ public awareness program.
- Refine and consider options to release pre-event information publicly, and take action accordingly.
- Obtain DNI approval of public disclosure to mitigate adverse effects on sensitive and ongoing prevention operations such as intelligence gathering, surveillance, etc.
- Share prompt and actionable messages, to include NTAS alerts, with the public and other stakeholders, as appropriate, to aid in the prevention of imminent or follow-on terrorist attacks.
- Review post-event public message plan and consider publicly releasing pre-event information to mitigate the effects of a successful attack on the populace.
- Leverage all appropriate communication means such as the Integrated Public Alert and Warning System (IPAWS) and social media.

**PLANNING**

**Description:** Conduct a systematic process engaging the whole community, as appropriate, in the development of executable strategic, operational and/or community-based approaches to meet defined objectives.

**Exhibit 8: Target Objectives for Planning**

<table>
<thead>
<tr>
<th>Row</th>
<th>Target Objectives for Planning</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Identify critical objectives based on the planning requirement, provide a complete and integrated picture of the sequence and scope of the tasks to achieve the objectives, and ensure the objectives are implementable within the time frame contemplated within the plan using available resources for prevention-related plans.</td>
</tr>
<tr>
<td>2</td>
<td>Develop and execute appropriate courses of action in coordination with Federal, state, local, and private sector entities in order to prevent an imminent terrorist attack within the United States.</td>
</tr>
</tbody>
</table>

In the context of Prevention, planning includes crisis action planning and development of options upon discovery of credible information about an imminent threat to the homeland or to prevent follow-on attacks. Both activities may occur in a time-constrained environment, potentially with several unknown factors.

**Critical Tasks**

- Initiate a time sensitive, flexible planning process that builds on existing plans and incorporates real-time intelligence.
• Make appropriate assumptions to inform decision makers and counterterrorism professionals’ actions to prevent imminent attacks on the homeland.

• Evaluate current intelligence and coordinate the development of options as appropriate.

• Identify possible terrorism targets and vulnerabilities.

• Identify law enforcement, intelligence, diplomatic, private sector, economic, and/or military options designed to prevent, deter, or disrupt imminent terrorist attacks in the homeland.

• Present courses of action to decision makers to prevent, deter, or disrupt imminent attacks in the homeland.

OPERATIONAL COORDINATION

Description: Establish and maintain a unified and coordinated operational structure and process that appropriately integrates all critical stakeholders and supports execution of core capabilities.

Exhibit 9: Target Objectives for Operational Coordination

<table>
<thead>
<tr>
<th>Row</th>
<th>Target Objectives for Operational Coordination</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Execute operations with functional and integrated communications among appropriate entities to prevent initial or follow-on terrorist attacks within the United States in accordance with established protocols.</td>
</tr>
</tbody>
</table>

This is the capability to conduct actions and activities that enable senior decision makers to determine appropriate courses of action and to provide oversight for complex operations to achieve unity of effort and effective outcomes. Effective operational coordination provides for cohesive command and control in order to ensure coordination of the investigative, intelligence and other activities in the face of an imminent terrorist threat or following an act of terrorism committed in the homeland.

In the context of Prevention, this includes efforts to coordinate activities across and among all levels of government and with critical nongovernmental or private sector partners. This capability involves national and field level operations and intelligence centers, as well as on-scene command and control centers, that coordinate multi-agency efforts to prevent imminent threats or conduct law enforcement investigative and response activities after an act of terrorism.

Critical Tasks

• Collaborate with all relevant stakeholders.

• Ensure clear lines and modes of communication among participating organizations and jurisdictions, both horizontally and vertically.

• Define and communicate clear roles and responsibilities relative to courses of action.

• Integrate and synchronize actions of participating organizations and jurisdictions to ensure unity of effort.
• Determine priorities, objectives, strategies, and resource allocations.

• Coordinate activities across and among all levels of government and with critical nonprofit and private sector partners to prevent imminent terrorist threats and/or conduct law enforcement investigative and response activities after an act of terrorism.

5.0 COORDINATING STRUCTURES

Coordinating structures support the delivery of core preparedness capabilities. A coordinating structure is composed of representatives from multiple departments or agencies, public and/or private sector organizations, or a combination of the preceding, which is able to facilitate the preparedness and delivery of capabilities. Coordinating structures ensure ongoing communication and coordination among Federal agencies and corresponding state and local authorities and nonprofit and private sector organizations, as applicable. Coordinating structures bring together capabilities to address requirements of the mission area and function both as a readiness tool and as an operational tool.

Coordinating structures facilitate problem solving, improve access to resources and foster coordination and information sharing. Individual departments or agencies with unique missions in the Prevention mission area bring additional capabilities to bear through these structures. The structures outlined below play a key role in delivering the Prevention core capabilities.

Coordinating structures can function on multiple levels, to include national-level coordinating structures, such as DHS’s National Operations Center (NOC), the FBI’s Strategic Information Operations Center, the Office of the Director of National Intelligence’s (ODNI’s) National Counterterrorism Center, DoD’s National Military Command Center, the national JTTF, and others. Field coordinating structures, such as the JTTFs, FBI FIGs, state and major urban area fusion centers, state and local counterterrorism and intelligence units, and others also play a critical role as coordinating structures for the prevention of imminent acts of terrorism. These coordinating structures are scalable, flexible, and adaptable. Staffing and location can be tailored to address specific terrorist threats.

6.0 NATIONAL LEVEL COORDINATING STRUCTURES

The National Security Council (NSC)

The NSC is the principal forum for consideration of national security policy issues requiring Presidential determination. The NSC shall advise and assist the President in integrating all aspects of national security policy as it affects the United States—domestic, foreign, military, intelligence, and economic. Along with its subordinate committees, the NSC shall be the President’s principal means for coordinating executive departments and agencies in the development and implementation of national security policy. In an imminent threat situation, NSC members may evaluate and recommend options to marshal a wide range of Federal Government capabilities to prevent initial or follow-on attacks on the homeland.

---

8 PPD-1
Core Capabilities: Public Information and Warning; Operational Coordination; Planning

**National Counterterrorism Center (NCTC)**

The NCTC is an ODNI-led coordinating structure that leads the Nation’s efforts to combat terrorism by analyzing the threat; sharing that information with Federal, state, and local partners; and integrating all of the instruments of national power. NCTC is the primary organization for analysis and integration of all intelligence pertaining to terrorism and counterterrorism. NCTC also conducts strategic and operational planning for integrated counterterrorism activities.\(^9\) Intelligence and information sharing is accomplished via a collaborative report of finished intelligence that updates the Presidential Daily Brief and daily National Terrorism Bulletin. NCTC maintains operational coordination of the repository of information on international terrorist identities and provides authoritative database supporting the Terrorist Screening Center and the U.S. Government watchlisting system. NCTC also provides expertise and analysis of key terrorism-related issues.

Core Capabilities: Intelligence and Information Sharing; Planning

**National Operations and Coordination Centers**

National Operations and Coordination Centers facilitate time-sensitive incident management coordination, situational awareness, and the sharing of critical intelligence and information. These centers provide valuable support in the prevention of terrorism and may be comprised of representatives from Federal, state, and/or local entities. Examples include DHS’s NOC, the FBI’s Strategic Information and Operations Center (SIOC), DoD’s National Military Command Center (NMCC), and NCTC’s Counterterrorism Watch. Many National Operations and Coordination Centers operate 24 hours a day, seven days a week, 365 days a year.

Core Capabilities: Intelligence and Information Sharing; Operational Coordination

**National Joint Terrorism Task Force (NJTTF)**

The NJTTF coordinates the efforts of all JTTFs and facilitates the coordination of Federal, state, and local agencies acting as an integrated force to combat terrorism on a national and international scale. The NJTTF exchanges information, analyzes data, and plans anti-terrorism strategies. The NJTTF is housed at NCTC, where it performs its mission while also working with NCTC personnel from the law enforcement, intelligence, homeland security, defense, diplomatic, and public safety sectors who work together every day in the global war on terrorism.

Core Capabilities: Intelligence and Information Sharing; Operational Coordination

**Terrorist Screening Center (TSC)**

The TSC supports Federal, state, and local law enforcement agencies and some foreign governments that conduct terrorist screening by making the Terrorist Screening Database (TSDB) information available to them for screening purposes. TSC’s 24-hour call center also

\(^9\)National Security Act of 1947 Section 119 (50 USC S 404o) and Quadrennial Homeland Security Report (p.A3)
supports agencies’ terrorist screening processes by determining whether the person being screened is an identity match to the TSDB. TSC supports terrorism screening at a variety of Federal agencies, has also made Terrorist Identities Information accessible through the National Crime Information Center system to law enforcement officers, including 870,000 state and local officers nationwide, adding those resources to the fight against terrorism. The TSC’s primary responsibility is to ensure that the identity data that is already known to the U.S. Government is held in one location where it can be queried by those who need it, including Federal, state, and local law enforcement and border control officers in certain foreign countries. While doing so, the TSC is dedicated to ensuring that data is maintained in a manner consistent with protecting privacy and civil liberties.

- Core Capabilities: Intelligence and Information Sharing; Screening, Search and Detection; Operational Coordination

**Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)**

The NSI is a collaborative effort led by the Department of Justice (DOJ), Bureau of Justice Assistance in partnership with DHS, FBI, and state and local law enforcement partners. The NSI provides law enforcement with another tool to help prevent terrorism and other related criminal activity by establishing a national capacity for gathering, documenting, processing, analyzing, and sharing SAR information. The NSI establishes a standardized process—which includes stakeholder outreach, privacy protections, training, and enabling technology—to identify and report suspicious activity in jurisdictions across the country, and serves as the unified focal point for sharing SAR information. There are multiple options for entry of the SAR data, to include the Shared Space and eGuardian, which allows FBI JTTFs and fusion centers to seamlessly access and share SAR information. The NSI also includes comprehensive training for chief executives, analysts, front line officers, and public safety partners on SAR awareness, as well as how to identify and report pre-incident terrorism indicators while ensuring protection of privacy, civil rights, and civil liberties.

- Core Capabilities: Intelligence and Information Sharing; Public Information and Warning

**FIELD LEVEL COORDINATING STRUCTURES:**

**Joint Operations Center (JOC)**

The JOC is a forward operating, interagency investigative and intelligence operations center led by the FBI. The JOC operates only during a crisis situation or for special events that require additional coordination between participating entities. The JOC coordinates law enforcement investigative, intelligence, and operational response activities in response to a threat or terrorist incident, major criminal investigation, or special event, including a National Special Security Event (NSSE). In order to provide successful investigative case management, the JOC may be activated and operational at any point in the response to a threat or incident.

---

Joint Terrorism Task Forces

JTTFs are FBI led multi-jurisdictional task forces established to conduct terrorism-related investigations and are based in 104 cities nationwide. JTTFs focus primarily on terrorism-related issues, with specific regard to terrorism investigations with local, regional, national, and international implications. Investigations conducted by JTTFs are focused on known threat actors or identified individuals who meet the thresholds established in accordance with the Attorney General Guidelines for Domestic FBI Operations to initiate assessments or investigations.

JTTFs respond to WMD threats, bringing the law enforcement, homeland security, and intelligence communities’ counter-WMD capabilities to bear, ensuring that the whole of government is ready to respond to WMD threats if/when they emerge. This involves the development of comprehensive plans and policy at the strategic and operational levels that inform leaders, decision makers, and counterterrorism professionals about specific responsibilities and courses of action.

JTTFs conduct terrorism related investigations and resolve reports of possible terrorism activity submitted from the public via the FBI's Guardian system and the FBI's e-Guardian system, which is one of the reporting mechanisms for law enforcement agencies to share SAR information within the NSI.

State and Major Urban Area Fusion Centers

Fusion centers serve as focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information between the Federal Government and state, local, and private sector partners. 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 protection, and private sector security personnel to understand local implications of national intelligence, thus enabling officials to better protect their communities. Fusion centers provide interdisciplinary expertise and situational awareness to inform decision-making at all levels of government. They conduct analysis and facilitate information sharing while assisting law enforcement and homeland security partners in preventing, protecting against, and responding to crime and terrorism. Fusion centers 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, and connectivity to Federal systems, technology, and grant funding.

Fusion centers contribute to the Information Sharing Environment (ISE) through their role in receiving threat information from the Federal Government; analyzing that information in the context of their local environment; disseminating that information to local agencies; and gathering tips, leads, and SAR from local agencies and the public. Fusion centers receive information from a variety of sources, including SAR from stakeholders within their
jurisdictions, as well as Federal information and intelligence. They analyze the information and
develop relevant products to disseminate to their customers. These products assist homeland
security partners at all levels of government to identify and address immediate and emerging
threats. With timely, accurate information on potential terrorist threats, fusion centers can
directly contribute to and inform investigations initiated and conducted by Federal entities, such
as the JTTFs.

- Core Capabilities: Intelligence and Information Sharing; Screening, Search, and
  Detection; Public Information and Warning

**Field-Level Operational Entities**

Field-Level Operational Entities may be deployed to deliver specialized capabilities in
time-sensitive situations to prevent imminent acts of terrorism, and may be comprised of any
combination of representatives from Federal, state, and local agencies. These entities can provide
deterrent presence and detection capabilities, and introduce an element of unpredictability to
disrupt potential terrorist planning activities. Field-Level Operational Entities are coordinated
through established procedures and protocols to improve interagency communications and to
maximize Federal, state, and local resource delivery, providing an effective defense against
terrorism.

- Core Capabilities: Screening, Search and Detection; Interdiction and Disruption;
  Forensics and Attribution

**State and Local Intelligence and Analytic Entities**

State and Local Intelligence and Analytic Entities strengthen and coordinate the
intelligence and information sharing capabilities and operations of Federal, state, and local law
enforcement agencies to prevent and disrupt terrorism and criminal activities while protecting
privacy, civil rights, and civil liberties. Complementing the national network of fusion centers
and JTTFs, these entities represent and support locally-led counterterrorism, intelligence, and
information sharing efforts. This may include supporting Federal investigations, intelligence
collection and analysis activities, intelligence led policing efforts, and community engagement
for the purpose of countering violent extremism. While locally-led, these efforts are designed to
support the prevention of terrorism threats and incidents in the homeland as well as national and
transnational crime.

- Core Capabilities: Intelligence and Information Sharing; Screening, Search and
  Detection; Interdiction and Disruption

---

11 These intelligence and analytic entities include state and local intelligence units, real-time crime analysis centers,
and other law enforcement or homeland security investigative and analytic centers that have not been designated as
fusion centers by state governments.
Exhibit 10 depicts how the coordinating structures identified in the National Prevention Framework will work together at all levels to prevent an imminent terrorist attack in the United States. In many cases, individuals, community organizations, private and nonprofit sector partners, or state and local entities may be the first to discover an imminent terrorist threat. Other times, the initial discovery of an imminent threat may occur at the Federal level. In all cases, the prevention coordinating structures outlined above will deliver appropriate capabilities in a coordinated and timely manner.

6.0 GUIDANCE FOR THE DEVELOPMENT OF OPERATIONAL PLANS

This section supports the planning core capability by providing guidance on the development of Federal, state, and local operational plans that support the National Prevention Framework. A plan is an explanation of anticipated actions that provides a starting point for operations. It provides three main benefits: (1) it allows jurisdictions to influence the course of events during an imminent threat by determining in advance the actions, policies, and processes.

* Situation Dependent: Any Individual or Local, State, or Federal Official May Be the First to Discover Intelligence or Operational Information Warning of an Imminent Threat.

---

12 This is not an exhaustive list of the coordinating structures for prevention. Other coordinating structures may also play a role, depending on the nature of the threat or incident.
that will be followed; (2) it contributes to unity of effort by providing a common blueprint for activity in the event of a crisis; and (3) it guides preparedness activities.

**Criteria for Successful Operational Planning**

Federal, state, local, and private sector prevention plans supporting the National Prevention Framework should meet certain criteria:

- Collaboration with all relevant stakeholders.
- Understand the situation expected during the intended operation.
- A detailed concept of operations that explains how prevention operations during an imminent threat will be executed in a coordinated fashion.
- A description of critical tasks and responsibilities.
- Resource, personnel, and sourcing requirements.
- Specific provisions for the rapid integration of resources and personnel.
- Account for multiple, geographically dispersed attacks of an extended nature.
- Explain how prevention plans may be executed simultaneously with other plans.

It is important to recognize that planning is an iterative process. Plans will need to be revised after exercises and real-world incidents.

**Federal Interagency Operational Plan**

PPD-8 requires a Federal Interagency Operational Plan to support the National Prevention Framework. The Interagency Operational Plan should leverage current and past planning efforts to cover threats that exceed the capabilities of state and local governments, such as CBRNE threats that involve multiple jurisdictions, states, regions, or the entire Nation.

The base portion of the Federal Interagency Operational Plan for Prevention shall include:

- Threat overview.
- Planning assumptions.
  - An imminent terrorist attack in the United States will be the top priority for the U.S. Government and appropriate Federal departments and agencies will need to respond on short notice.
  - The capabilities of individuals and households, communities and community organizations, private and nonprofit sector, and state and local entities will play a critical role in preventing an imminent terrorist attack.
  - A terrorist attack will occur at any time of day with little or no warning and may involve single or multiple geographic areas.
  - Multiple, near simultaneous terrorist attacks will exceed the capabilities of any one entity.
  - A WMD terrorist attack will result in mass casualties.
WORKING DRAFT—NATIONAL PREVENTION FRAMEWORK

- Concept of operations.
  - Capability modules that detail critical tasks for each capability; supporting and supported responsibilities for each capability; and resource, personnel, and sourcing requirements for each capability.
  - Specific provisions for the rapid integration of resources and personnel through the coordinating structures identified in the Framework.

- Explanation of how the Federal Interagency Operational Plan for Prevention relates to other mission areas, as appropriate.

The Federal Interagency Operational Plan for Prevention will address unique planning considerations for terrorist threats identified in the SNRA:

- Chemical.
- Biological.
- Radiological/Nuclear.
- Explosives/Armed Assault.

The Federal Interagency Operational Plan for Prevention should serve as the foundation for the development of pre-scripted mission assignments (PSMAs) captured in department- and agency-level operational plans. PSMAs facilitate timely execution of prevention operations by outlining mutually agreed upon tasks to be performed by the assigned Federal agency. Valuable PSMAs specify the type, scope, and duration of the mission.

State, Local, and Tribal Prevention Planning

Comprehensive Preparedness Guide (CPG) 101 provides guidance for developing emergency operations plans at the state and local level. It promotes a common understanding of the fundamentals of risk-informed planning and decisionmaking to help planners produce integrated, coordinated, and synchronized plans. Even though CPG 101 was designed for emergency management planners, certain elements of CPG 101—such as the basics of planning, format and function of planning, and planning processes—apply to prevention planning at the state and local level.13 The Federal Government can also leverage this guidance, as appropriate.

State and local officials are strongly encouraged to develop a prevention plan in support of the National Prevention Framework. Prevention plans should explain how stakeholders will deliver the Prevention core capabilities and execute the critical tasks outlined in Section 4.0. Additionally, all plans should identify the type of tasks, scope of capabilities, and timeframe of support that each jurisdiction may need from the Federal Government, including any incident specific considerations.

---

13 CPG 502 also provides state and major urban area fusion center and emergency operations center (EOC) officials with guidance for the coordination among fusion centers and EOCs. It outlines the roles of fusion centers and EOCs and provides steps by which these entities can work together to share information and intelligence on an ongoing basis.
7.0 FRAMEWORK MAINTENANCE AND REVIEW CYCLE

The first edition of the National Prevention Framework is to be reviewed within 18 months of release. The Framework will be reviewed and updated, as appropriate, every four years thereafter.

DHS, DOJ, and ODNI will coordinate and oversee the review and maintenance process for the National Prevention Framework. The revision process includes developing or updating any documents necessary to carry out capabilities. This Framework is reviewed at least annually in order to accomplish the following:

- Assess and update core capabilities in support of prevention goals and objectives.
- Ensure that it adequately reflects the organization of responsible entities.
- Ensure that it is consistent with the other four mission areas.
- Update processes based on changes in the national threat environment.
- Incorporate lessons learned and effective practices from day-to-day operations, exercises, and actual incidents and alerts.
- Reflect progress in the Nation’s prevention mission activities, as well as changes to national priorities and guidance, critical tasks, or national capabilities.

As changes are warranted, periodic updates to the National Prevention Framework will be issued. The types of developments that merit a periodic update include new laws, Executive Orders, Presidential directives, regulations, and procedural changes to Framework activities based on real-world incidents or exercise experiences.

**Types of Changes.** Changes include the addition of new or supplementary material and deletions. No proposed change can contradict or override the authorities of departments or agencies with regard to the direction, conduct, control, planning, organization, equipment, training, exercises, or other activities concerning domestic counterterrorism intelligence and law enforcement activities.¹⁴

**Coordination and Approval.** While DHS, DOJ, and ODNI are the lead Federal departments and agencies for the National Prevention Framework development, any Federal department or agency with roles and responsibilities under this Framework may propose a change. The review process will engage the whole community to solicit feedback and recommendations. DHS is responsible for coordinating the review and approval of all proposed modifications with Prevention partners, as appropriate. Policy changes will be coordinated and approved through the Counterterrorism Security Group (CSG).

**Notice of Change.** An official Notice of Change will be issued for each interim revision to this Framework. After publication, the modifications will be considered part of the National Prevention Framework for planning purposes pending a formal revision and reissuance of the entire document. Interim changes can be further modified or updated using this process. Periodic updates resulting from the annual review process do not require the formal Notice of Change.

¹⁴ PPD-8
**Distribution.** Official Notices of Change will be distributed to Federal, state, and local
government entities as well as specific private sector partners. Notices of Change to other
organizations will be provided upon request.

**Reissuance.** DHS, DOJ, and ODNI will coordinate full reviews and updating of this
Framework every four years or more frequently, if directed by the President. DHS, DOJ, and
ODNI will distribute revised documents for review and concurrence.