

PRESIDENTIAL POLICY DIRECTIVE/PPD-8
WORKING DRAFT—NATIONAL PREVENTION FRAMEWORK
REVIEW PACKAGE

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> or send an e-mail to PPD8-Engagement@fema.gov.

**WORKING DRAFT—NATIONAL PREVENTION FRAMEWORK
FOR NATIONAL REVIEW
20120302, 0800 EST**

1.0 INTRODUCTION

The National Prevention Framework (Framework) describes what the whole community—from observant citizens to senior leaders in government—must do upon discovery of intelligence or information regarding an imminent threat to the homeland in order to thwart an initial or follow-on terrorist attack.

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.

Presidential Policy Directive 8 (PPD-8) was designed to establish a capability-based level of national preparedness against all threats and hazards from prevention through recovery. PPD-8 directs “systematic preparation for the threats that pose the greatest risk to the security of the Nation, including acts of terrorism, cyber attacks, pandemics, and catastrophic natural disasters.” In particular, PPD-8 directs the development of a National Prevention Framework to prevent “imminent” terrorist attacks on U.S. soil.

The Framework helps achieve the National Preparedness Goal of a secure and resilient Nation that is optimally prepared to prevent an imminent terrorist attack within the United States.¹

This Framework applies to leaders and practitioners at all levels of government; private- and non-profit sector partners; and individuals. The Framework will benefit the whole community by:

- Providing guidance to prevent, avoid, or stop a threatened or actual act of terrorism.
- Aligning key roles and responsibilities to deliver Prevention capabilities in time-sensitive situations.
- Describing coordinating structures that enable all stakeholders to work together.
- Laying the foundation for further operational coordination and planning that will synchronize Prevention efforts within the whole community and across the protection, mitigation, response, and recovery focus areas.

2.0 SCOPE

The United States carries out many programs and operations to prevent terrorism at home and abroad. These programs help meet the President’s goals to: defeat al-Qa’ida and its affiliates and adherents; prevent terrorist development, acquisition, and use of weapons of mass destruction; eliminate terrorist safe havens; build enduring counterterrorism partnerships; and counter al-Qa’ida’s ideology.

¹ The National Preparedness Goal is located at <http://www.fema.gov/ppd8>.

38 Terrorism prevention should be conducted as far from its intended target as possible.
39 Ideally, terrorism is addressed at its root, by countering radicalization toward a violent extremist
40 ideology. Therefore, it is preferable to deter terrorist plots, to thwart or counter emerging terrorist
41 plots at the earliest stages, and, if other efforts fail, to detect, disrupt, and interdict ongoing
42 terrorist activity as far from the intended target as possible.²

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

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

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

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

70 **RISK BASIS**

71 The Secretary of Homeland Security led an interagency effort to conduct a Strategic
72 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>.

73 greatest risk to the Nation. In turn, the National Preparedness Goal identifies the core capabilities
 74 essential to address these risks in each of the five preparedness mission areas. This Framework
 75 addresses delivery of the core capabilities required to address the following adversarial/human-
 76 caused risks.

77

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

Row	Threat Type	National-level Event Description
1	Aircraft as a Weapon	A hostile non-State actor(s) crashes a commercial or general aviation aircraft into a physical target within the United States
2	Armed Assault	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
3	Biological Terrorism Attack (non-food)	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
4	Chemical/Biological Food Contamination Terrorism Attack	A hostile non-State actor(s) disperses a biological or chemical agent into food supplies within the U.S. supply chain
5	Chemical Terrorism Attack (non-food)	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
6	Explosives Terrorism Attack	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
7	Nuclear Terrorism Attack	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
8	Radiological Terrorism Attack	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)

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

83 **The Prevention mission area is focused exclusively on terrorist threats; the other**
 84 **four preparedness mission areas are “all hazards.”** In addition to the terrorist threats
 85 identified above, the SNRA identifies a range of hazards (natural disasters, pandemics,
 86 technological accidents, and cyber attacks) that pose a risk to the safety and security of our
 87 Nation. These hazards, and the core capabilities required to address them, are addressed in the
 88 other four preparedness mission areas, as appropriate.

89 All levels of government, private and non-profit sector organizations, communities, and
90 households should assess their particular risks to identify capability requirements and prioritize
91 their preparedness efforts.

92 INTENDED AUDIENCE

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

103 The Framework also provides guidance to intelligence and law enforcement professionals
104 on how existing structures; such as the Federal Bureau of Investigation’s (FBI’s) JTTFs, state
105 and major urban area fusion centers, and state and local counterterrorism and intelligence units;
106 can collaborate and prioritize their efforts to support the delivery of Prevention core capabilities.

107 Finally, the Framework is also for communities and citizens. It outlines the role of the
108 public in terrorism prevention, especially in reporting potentially terrorism related or suspicious
109 activities. The Framework explains how the general public and private sector may serve as a
110 force multiplier for law enforcement in terrorism prevention.

111 GUIDING PRINCIPLES FOR PREVENTION

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

117 **(1) The whole community has a key role to play in terrorism prevention through**
118 **engaged partnership.** The prevention of terrorism is a shared responsibility among the various
119 Federal, state, local, and non-profit and private sector entities that comprise the whole
120 community.⁴ Each level of government must play a prominent role in building capabilities,
121 developing plans, and conducting exercises to prepare to prevent an imminent terrorist attack. In
122 addition, individuals, non-profit and private sector entities, and international partners can all
123 provide critical assistance.

124 **(2) Core capabilities are scalable, flexible, and adaptable and executed as needed to**
125 **address the full range of threats as they evolve.** Depending on the nature, scope, or location of
126 the threat, officials from all levels of government may elect to execute some or all core
127 capabilities covered in this Framework. The coordinating structures outlined in the Framework
128 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.

129 **(3) The whole community builds and maintains the core capabilities in order to**
130 **execute them either before an attack, based on knowledge of an imminent threat or after an**
131 **incident to prevent follow-on attacks and/or apprehend the adversary (i.e., readiness to**
132 **act).**

133 **RELATIONSHIP TO OTHER MISSION AREAS**

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

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

- 143 • **Protection.** Prevention and Protection are closely aligned. The Prevention mission
144 area focuses on those intelligence, law enforcement, and homeland security activities
145 which prevent an adversary from carrying out an attack within the United States.
146 Protection activities focus on decreasing the likelihood of an attack within the
147 homeland. Protection and Prevention share a number of common elements and rely
148 on many of the same core capabilities. Protection and Prevention processes described
149 in these frameworks are designed to operate simultaneously and to complimentary
150 with each other.
- 151 • **Mitigation.** The law enforcement, intelligence, and homeland security communities
152 play a significant role in Mitigation. Outreach and community involvement help to
153 establish and maintain strong ties with neighbors, businesses, academic institutions,
154 and critical infrastructure owners and operators. Intelligence-focused relationships
155 among Federal, state, and local law enforcement, intelligence and homeland security
156 entities, and with the public and private sector, academia, and other community
157 organizations facilitate information sharing. In turn, this creates more opportunities to
158 thwart acts of terrorism and to lessen the effects of large-scale, man-made
159 catastrophes should they occur. Through these dialogues, communities may better
160 detect and deter specific threats and mitigate vulnerabilities. They may also develop
161 new ways of reducing risks and reporting successful practices. Finally, through
162 integrated and risk-informed planning efforts, law enforcement and homeland
163 security partners can help improve the whole community’s ability to avoid future loss
164 of life and property.

Exhibit 2: Core Capabilities by Preparedness Mission Area

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

166
167
168
169
170
171
172

- 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

173 of an imminent threat so that Response assets, to the extent practical and appropriate,
174 may be pre-positioned. Both Response and Recovery functions personnel will be
175 unable to access the scene of a terrorist attack until criminal investigators and
176 forensics teams finish their work. But, Prevention assets will provide Response and
177 Recovery personnel data concerning contamination in the impacted area which will
178 assist response and recovery activities. In many cases, Prevention will be working
179 simultaneously with Recovery in this regard.

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

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

192 **3.0 ROLES AND RESPONSIBILITIES**

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

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

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

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

213 **Local governments** provide front-line leadership for local law enforcement, fire, public
214 safety, environmental response, public health, and emergency medical services for all manner of
215 threats, hazards and emergencies. Local governments coordinate resources and capabilities

216 during critical incidents with neighboring jurisdictions, the State, and the private and non-profit
217 sectors.

218 **Local law enforcement agencies** are responsible for the preservation of peace, the
219 protection of life and property, the prevention of crime, and the arrest of violators of the law.
220 These agencies engage in community and interagency partnerships so as to identify and prevent
221 criminal acts to include terrorism and transnational threats.

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

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

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

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

250 **The Department of Justice**, under the Attorney General, has lead responsibility for
251 criminal investigations of terrorist acts or terrorist threats by individuals or groups inside the
252 United States, or directed at U.S. citizens or institutions abroad, as well as for related intelligence
253 collection activities within the United States, subject to the National Security Act of 1947, other
254 applicable law, Executive Order 12333, and Attorney General-approved procedures pursuant to
255 that Executive Order. Generally acting through the Federal Bureau of Investigation, the Attorney
256 General, in cooperation with other Federal departments and agencies engaged in activities to
257 protect national security, shall also coordinate the activities of the other members of the law
258 enforcement community to detect, prevent, preempt, and disrupt terrorist attacks against the
259 United States.

260 **The Secretary of Homeland Security** leads the Federal interagency in securing the
261 homeland against terrorism and other threats and hazards. The role of the Department of
262 Homeland Security (DHS) in preventing terrorism includes assessing and managing terrorism
263 risk; preventing terrorists from entering or remaining in the country; preventing acquisition of
264 WMD-related materials and/or weapons; preventing importation of weapons and weapons-
265 related materials through screening, search, detection, and interdiction; preventing the use of our
266 transportation systems for terroristic purposes; and interdicting terrorist activity within the
267 maritime, air, and land domains. DHS coordinates its actions with the interagency, and when
268 appropriate, coordinates interagency actions. Finally, DHS shares information on terrorist threats
269 with Federal, state, and local governments and private sector partners.

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

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

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

302 In accordance with the President’s intent as outlined in the National Security Strategy,
303 preventing a terrorist attack requires a whole of government approach. To that end, under the
304 National Prevention Framework, and consistent with existing law, Executive Orders, regulations

305 and policy, various **other Federal departments and agencies** may play primary, coordinating
 306 and/or supporting roles in the prevention of an imminent act of terrorism based on their
 307 authorities and resources and the nature of the threat or incident. While not called out
 308 individually, many Federal agencies and departments contribute greatly to the prevention effort.

309 **4.0 CORE CAPABILITIES**

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

317 **INTELLIGENCE AND INFORMATION SHARING**

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

326 **Exhibit 3: Target Objectives for Intelligence and Information Sharing**

Row	Target Objectives for Intelligence and Information Sharing
1	Anticipate and identify emerging and/or imminent threats through the intelligence cycle.
2	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.
3	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.

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

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

339 and develop and disseminate risk assessments and analysis of national intelligence to state, local,
 340 and private sector partners.

341 This capability relies on the analytical and information sharing capabilities of JTTFs and
 342 state and major urban area fusion centers during times of imminent threat, in accordance with
 343 existing laws, directives, and policies.⁵ It involves reprioritization and retasking of law
 344 enforcement and intelligence assets as necessary and appropriate. Amplifying information will
 345 also be obtained via law enforcement operations.

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

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

352 ***Critical Tasks***

- 353 • Planning and Direction: Establish the intelligence and information requirements of
 354 the consumer.
 - 355 ○ Rapidly reprioritize law enforcement and intelligence assets, as necessary and
 356 appropriate.
 - 357 ○ Engage with private sector partners in order to determine what intelligence
 358 and information assets may be available for reprioritization.
 - 359 ○ Request additional intelligence requirements via law enforcement deployment,
 360 questioning of witnesses and suspects, increased surveillance activity,
 361 community policing and outreach, etc.
- 362 • Collection: Gather the required raw data to produce the desired finished intelligence
 363 and information products.
 - 364 ○ Gather/collect information via law enforcement operations, suspicious activity
 365 reporting, surveillance, community engagement, and other activities and
 366 sources as necessary.
- 367 • Exploitation and Processing: Convert raw data into comprehensible forms that can be
 368 utilized to produce finished intelligence and information products.
- 369 • Analysis and Production: Integrate, evaluate, analyze, and prepare the processed
 370 information for inclusion in the finished product.
- 371 • Dissemination: Deliver finished intelligence and information products to the
 372 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>.

- 373 ○ When necessary, develop appropriately classified/unclassified products to
- 374 disseminate threat information to Federal, state, local, international, private
- 375 and nonprofit sector, and public partners.
- 376 ○ Adhere to mechanisms for safeguarding sensitive information, consistent with
- 377 Executive Order 13587.⁶
- 378 ● Evaluation and Feedback: Acquire continual feedback during the intelligence cycle
- 379 that aids in refining each individual stage and the cycle as a whole.
- 380 ● Continually assess threat information to inform continued prevention operations.

381 **SCREENING, SEARCH, AND DETECTION**

382 Description: Identify, discover, or locate imminent terrorist threats through active and

383 passive surveillance and search procedures. This may include the use of systematic examinations

384 and assessments, sensor technologies, or physical investigation and intelligence.

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

Row	Target Objectives for Screening, Search and Detection
1	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.
2	Initiate operations immediately to locate persons and networks associated with an imminent terrorist threat or act.
3	Conduct chemical, biological, radiological, nuclear, and explosive (CBRNE) search/detection operations in multiple locations and in all environments, consistent with established protocols.

386 In the context of Prevention, this capability includes the measures taken over-and-above

387 routine screening and detection activities to locate specific threats. These measures may be taken

388 in response to actionable intelligence that indicates potential targets, approach vectors, or type of

389 weapon to be used. They may also be taken to verify or characterize the threat of materials or

390 weapons that have already been located. Search and detection operations may be conducted with

391 limited or no intelligence about the location of the threat, which would require the Nation to

392 prioritize its search and detection resources.

393 This capability includes action taken to detect terrorist attacks in the planning, progress,

394 or execution phases. The whole community potentially has a role to play in this capability,

395 whether as an observant member of the public, the owner of critical infrastructure, or a law

396 enforcement agency. The fully developed capability means the whole community is optimally

397 prepared to quickly and effectively identify and locate terrorists and their means and methods of

398 terrorism to prevent an imminent terrorist act within the United States.

399 ***Critical Tasks***

- 400 ● 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.

- 401 • Develop and engage an observant Nation (individuals; families; communities; state,
402 and local partners; and industry).
- 403 • Screen persons, baggage, mail, cargo and conveyances using technical, non-technical,
404 intrusive, and non-intrusive means.
 - 405 ○ Consider additional measures for high risk persons, conveyances, or items.
- 406 • Conduct physical searches.
- 407 • Conduct CBRNE search/detection operations.
 - 408 ○ Conduct ambient and active detection of CBRNE agents.
 - 409 ○ Operate in a hazardous environment.
 - 410 ○ Conduct technical search/detection operations.
 - 411 ○ Conduct non-technical search/detection operations.
 - 412 ○ Consider deployment of Federal teams and capabilities to enhance state and
413 local efforts including use of incident assessment and awareness assets.
- 414 • Conduct medical surveillance.
- 415 • Employ wide-area search and detection assets in targeted region in concert with state
416 and local personnel or other Federal agencies (depending on threat).

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

420 **INTERDICTION AND DISRUPTION**

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

422 **Exhibit 5: Target Objectives for Interdiction and Disruption**

Row	Target Objectives for Interdiction and Disruption
1	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.
2	Conduct operations to render safe and dispose of CBRNE hazards in multiple locations and in all environments, consistent with established protocols.
3	Prevent terrorism financial/material support from reaching its target, consistent with established protocols.
4	Prevent terrorist acquisition of and the transfer of CBRNE materials, precursors, and related technology, consistent with established protocols.
5	Conduct tactical counterterrorism operations in multiple locations and in all environments, consistent with established protocols.

423 In the context of Prevention, this capability includes those interdiction and disruption
424 activities undertaken in response to specific, actionable intelligence that indicates the location of
425 a suspected weapon and/or perpetrator. It might also include in-extremis activities required when

426 a CBRNE device is encountered unexpectedly. Interdiction and disruption capabilities help to
 427 neutralize terrorist cells, operatives, and operations.

428 ***Critical Tasks***

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

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

444 **FORENSICS AND ATTRIBUTION**

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

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

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

450 Forensic examinations are critical to the process of attributing actions to individuals or
 451 entities. Attribution involves the fusion of all-source intelligence and information, including
 452 forensic evidence, into a confident conclusion about who is responsible for a pending threat or
 453 successful attack. The attribution process may differ depending on the type of attack. The United
 454 States must be able to identify the source of any type of attack, especially those types identified

455 in the SNRA. This capability is critical in preventing potential follow-on attacks and swiftly
456 developing options.

457 In the context of Prevention, this capability may need to be delivered in a time-
458 constrained or crisis environment. Execution of this capability would likely begin upon
459 discovery of trace evidence at locations where suspected weapons or perpetrators may have been
460 located, upon discovery of additional information on the current location of the threat, or upon an
461 adversary's claim of responsibility for an act of terrorism.

462 ***Critical Tasks***

- 463 • Conduct physical evidence analysis.
 - 464 ○ Process fingerprints.
 - 465 ○ Conduct toxicology.
 - 466 ○ Conduct materials analysis (e.g., paints, tapes, inks, glass, paper, and metals).
- 467 • Conduct chemical, biological, radiological, and nuclear (CBRN) material analysis.
 - 468 ○ Conduct trace organic and inorganic chemical analysis.
 - 469 ○ Conduct microbial forensics.
- 470 • Conduct biometric analysis.
- 471 • Conduct digital media and network exploitation.
- 472 • Conduct DNA analysis.
- 473 • Identify explosives.
- 474 • Assess capabilities of likely perpetrator(s).
- 475 • Deploy investigators and technical attribution assets to identify the attack
476 perpetrator(s).
- 477 • Interview witnesses, potential associates, and/or perpetrators if possible.
- 478 • Examine intelligence and forensics to refine/confirm attribution leads.
 - 479 ○ Gather samples in specific geographies or target locations.
 - 480 ○ Interpret and communicate attribution results and their significance to national
481 decision makers.
- 482 • Develop databases.

483 **PUBLIC INFORMATION AND WARNING**

484 **Description:** Deliver coordinated, prompt, reliable, and actionable terrorism-related
485 information to the whole community through the use of clear, consistent, accessible, and
486 culturally and linguistically appropriate methods to effectively relay information regarding any
487 imminent threat and, as appropriate, the actions being taken and the assistance being made
488 available.

Exhibit 7: Target Objectives for Public Information and Warning

Row	Target Objectives for Public Information and Warning
1	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.
2	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.

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

498 DHS leads the evaluation of terrorism vulnerabilities and coordinates with other Federal,
 499 state, local, and private entities to ensure the most effective response. The collection, protection,
 500 evaluation and dissemination of critical threat information to the American public, state and local
 501 governments, and the private sector is central to this task. This information is provided to the
 502 public, primarily through NTAS alerts.⁷ The NTAS system is designed to effectively
 503 communicate information about terrorist threats by providing timely, detailed information to the
 504 public, government agencies, first responders, airports and other transportation hubs, and the
 505 private sector. Depending on the nature of the threat, alerts may be sent to law enforcement,
 506 distributed to affected areas of the private sector, or issued more broadly to the public through
 507 both official and social media channels. Alerts may be broad, local, or sector specific. State and
 508 local governments may also choose to issue notices and alerts to their constituencies concerning
 509 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.

510 Should an NTAS alert be issued, fusion centers may be leveraged to disseminate time-
 511 sensitive NTAS alerts and associated preventive and protective measure information to fusion
 512 center partners and generate value-added analysis, information and intelligence within a local
 513 context.

514 ***Critical Tasks***

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

528 **PLANNING**

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

532 **Exhibit 8: Target Objectives for Planning**

Row	Target Objectives for Planning
1	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.
2	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.

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

537 ***Critical Tasks***

- 538 • Initiate a time sensitive, flexible planning process that builds on existing plans and
 539 incorporates real-time intelligence.

- 540 • Make appropriate assumptions to inform decision makers and counterterrorism
541 professionals’ actions to prevent imminent attacks on the homeland.
- 542 • Evaluate current intelligence and coordinate the development of options as
543 appropriate.
- 544 • Identify possible terrorism targets and vulnerabilities.
- 545 • Identify law enforcement, intelligence, diplomatic, private sector, economic, and/or
546 military options designed to prevent, deter, or disrupt imminent terrorist attacks in the
547 homeland.
- 548 • Present courses of action to decision makers to prevent, deter, or disrupt imminent
549 attacks in the homeland.

550 **OPERATIONAL COORDINATION**

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

554 **Exhibit 9: Target Objectives for Operational Coordination**

Row	Target Objectives for Operational Coordination
1	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.

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

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

566 ***Critical Tasks***

- 567 • Collaborate with all relevant stakeholders.
- 568 • Ensure clear lines and modes of communication among participating organizations
569 and jurisdictions, both horizontally and vertically.
- 570 • Define and communicate clear roles and responsibilities relative to courses of action.
- 571 • Integrate and synchronize actions of participating organizations and jurisdictions to
572 ensure unity of effort.

- 573 • Determine priorities, objectives, strategies, and resource allocations.
- 574 • Coordinate activities across and among all levels of government and with critical
- 575 nonprofit and private sector partners to prevent imminent terrorist threats and/or
- 576 conduct law enforcement investigative and response activities after an act of
- 577 terrorism.

578 **5.0 COORDINATING STRUCTURES**

579 Coordinating structures support the delivery of core preparedness capabilities. A

580 coordinating structure is composed of representatives from multiple departments or agencies,

581 public and/or private sector organizations, or a combination of the preceding, which is able to

582 facilitate the preparedness and delivery of capabilities. Coordinating structures ensure ongoing

583 communication and coordination among Federal agencies and corresponding state and local

584 authorities and nonprofit and private sector organizations, as applicable. Coordinating structures

585 bring together capabilities to address requirements of the mission area and function both as a

586 readiness tool and as an operational tool.

587 Coordinating structures facilitate problem solving, improve access to resources and foster

588 coordination and information sharing. Individual departments or agencies with unique missions

589 in the Prevention mission area bring additional capabilities to bear through these structures. The

590 structures outlined below play a key role in delivering the Prevention core capabilities.

591 Coordinating structures can function on multiple levels, to include national-level

592 coordinating structures, such as DHS’s National Operations Center (NOC), the FBI’s Strategic

593 Information Operations Center, the Office of the Director of National Intelligence’s (ODNI’s)

594 National Counterterrorism Center, DoD’s National Military Command Center, the national

595 JTTF, and others. Field coordinating structures, such as the JTTFs, FBI FIGs, state and major

596 urban area fusion centers, state and local counterterrorism and intelligence units, and others also

597 play a critical role as coordinating structures for the prevention of imminent acts of terrorism.

598 These coordinating structures are scalable, flexible, and adaptable. Staffing and location can be

599 tailored to address specific terrorist threats.

600 **NATIONAL LEVEL COORDINATING STRUCTURES**

601 ***The National Security Council (NSC)***

602 The NSC is the principal forum for consideration of national security policy issues

603 requiring Presidential determination. The NSC shall advise and assist the President in integrating

604 all aspects of national security policy as it affects the United States—domestic, foreign, military,

605 intelligence, and economic. Along with its subordinate committees, the NSC shall be the

606 President’s principal means for coordinating executive departments and agencies in the

607 development and implementation of national security policy.⁸ In an imminent threat situation,

608 NSC members may evaluate and recommend options to marshal a wide range of Federal

609 Government capabilities to prevent initial or follow-on attacks on the homeland.

⁸ PPD-1

- 610 • Core Capabilities: Public Information and Warning; Operational Coordination;
611 Planning

612 ***National Counterterrorism Center (NCTC)***

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

- 624 • Core Capabilities: Intelligence and Information Sharing; Planning

625 ***National Operations and Coordination Centers***

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

- 633 • Core Capabilities: Intelligence and Information Sharing; Operational Coordination

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

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

- 642 • Core Capabilities: Intelligence and Information Sharing; Operational Coordination

643 ***Terrorist Screening Center (TSC)***

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

⁹National Security Act of 1947 Section 119 (50 USC S 404o)and Quadrennial Homeland Security Report (p.A3)

647 supports agencies' terrorist screening processes by determining whether the person being
 648 screened is an identity match to the TSDB. TSC supports terrorism screening at a variety of
 649 Federal agencies, has also made Terrorist Identities Information accessible through the National
 650 Crime Information Center system to law enforcement officers, including 870,000 state and local
 651 officers nationwide, adding those resources to the fight against terrorism. The TSC's primary
 652 responsibility is to ensure that the identity data that is already known to the U.S. Government is
 653 held in one location where it can be queried by those who need it, including Federal, state, and
 654 local law enforcement and border control officers in certain foreign countries. While doing so,
 655 the TSC is dedicated to ensuring that data is maintained in a manner consistent with protecting
 656 privacy and civil liberties.

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

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

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

- 673 • Core Capabilities: Intelligence and Information Sharing; Public Information and
 674 Warning

675 **FIELD LEVEL COORDINATING STRUCTURES:**

676 *Joint Operations Center (JOC)*

677 The JOC is a forward operating, interagency investigative and intelligence operations
 678 center led by the FBI. The JOC operates only during a crisis situation or for special events that
 679 require additional coordination between participating entities. The JOC coordinates law
 680 enforcement investigative, intelligence, and operational response activities in response to a threat
 681 or terrorist incident, major criminal investigation, or special event, including a National Special
 682 Security Event (NSSE). In order to provide successful investigative case management, the JOC
 683 may be activated and operational at any point in the response to a threat or incident.¹⁰

¹⁰ FBI Public Web site, <http://www.fbi.gov/>

- 684 • Core Capabilities: Intelligence and Information Sharing; Screening, Search and
- 685 Detection; Interdiction and Disruption; Forensics and Attribution; Public Information
- 686 and Warning; Operational Coordination; Planning

687 *Joint Terrorism Task Forces*

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

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

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

- 704 • Core Capabilities: Intelligence and Information Sharing; Screening, Search and
- 705 Detection; Interdiction and Disruption; Forensics and Attribution; Public Information
- 706 and Warning; Operational Coordination

707 *State and Major Urban Area Fusion Centers*

708 Fusion centers serve as focal points within the state and local environment for the receipt,
 709 analysis, gathering, and sharing of threat-related information between the Federal Government
 710 and state, local, and private sector partners. Located in states and major urban areas throughout
 711 the country, fusion centers are uniquely situated to empower front-line law enforcement, public
 712 safety, fire service, emergency response, public health, critical infrastructure protection, and
 713 private sector security personnel to understand local implications of national intelligence, thus
 714 enabling officials to better protect their communities. Fusion centers provide interdisciplinary
 715 expertise and situational awareness to inform decision-making at all levels of government. They
 716 conduct analysis and facilitate information sharing while assisting law enforcement and
 717 homeland security partners in preventing, protecting against, and responding to crime and
 718 terrorism. Fusion centers are owned and operated by state and local entities with support from
 719 Federal partners in the form of deployed personnel, training, technical assistance, exercise
 720 support, security clearances, and connectivity to Federal systems, technology, and grant funding.

721 Fusion centers contribute to the Information Sharing Environment (ISE) through their
 722 role in receiving threat information from the Federal Government; analyzing that information in
 723 the context of their local environment; disseminating that information to local agencies; and
 724 gathering tips, leads, and SAR from local agencies and the public. Fusion centers receive
 725 information from a variety of sources, including SAR from stakeholders within their

726 jurisdictions, as well as Federal information and intelligence. They analyze the information and
 727 develop relevant products to disseminate to their customers. These products assist homeland
 728 security partners at all levels of government to identify and address immediate and emerging
 729 threats. With timely, accurate information on potential terrorist threats, fusion centers can
 730 directly contribute to and inform investigations initiated and conducted by Federal entities, such
 731 as the JTTFs.

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

734 ***Field-Level Operational Entities***

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

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

745 ***State and Local Intelligence and Analytic Entities¹¹***

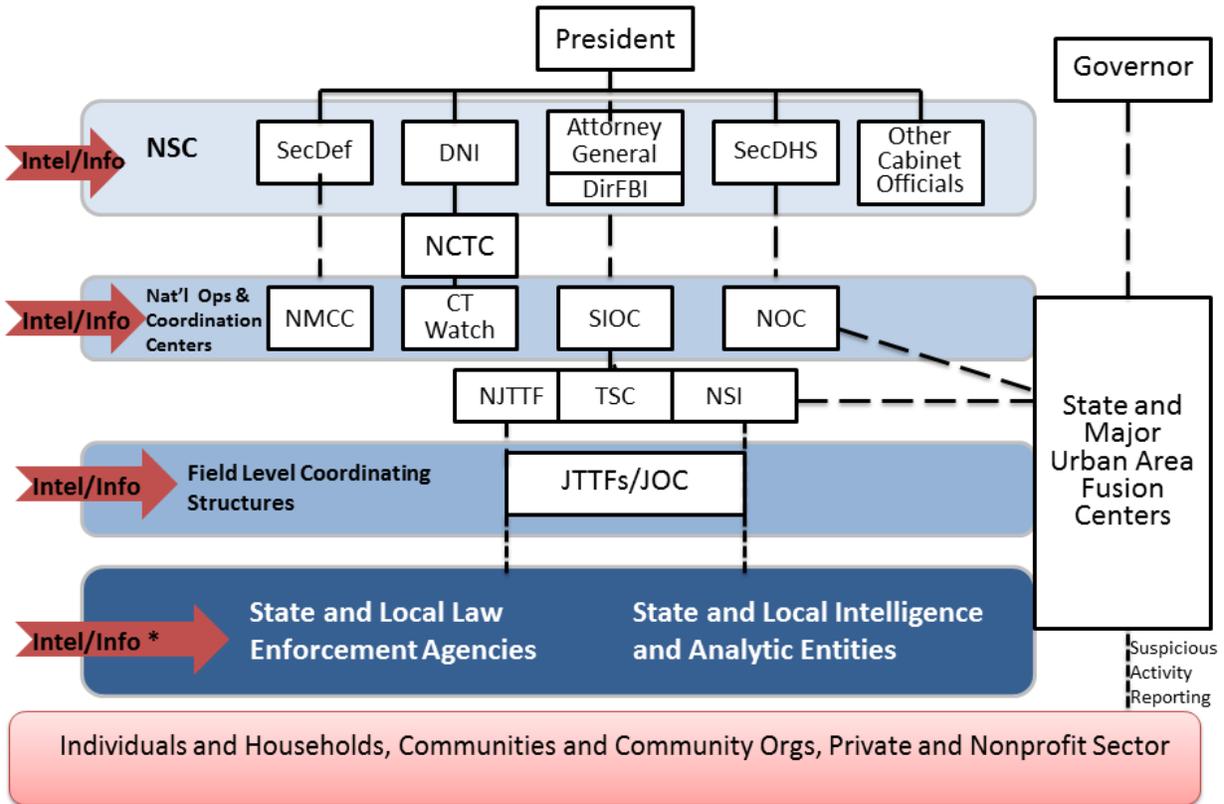
746 State and Local Intelligence and Analytic Entities strengthen and coordinate the
 747 intelligence and information sharing capabilities and operations of Federal, state, and local law
 748 enforcement agencies to prevent and disrupt terrorism and criminal activities while protecting
 749 privacy,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

- 756 • Core Capabilities: Intelligence and Information Sharing; Screening, Search and
 757 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.

758

Exhibit 10: Prevention Coordinating Structures



*** 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.**

759

760 Exhibit 10 depicts how the coordinating structures identified in the National Prevention
 761 Framework will work together at all levels to prevent an imminent terrorist attack in the United
 762 States.¹² In many cases, individuals, community organizations, private and nonprofit sector
 763 partners, or state and local entities may be the first to discover an imminent terrorist threat. Other
 764 times, the initial discovery of an imminent threat may occur at the Federal level. In all cases, the
 765 prevention coordinating structures outlined above will deliver appropriate capabilities in a
 766 coordinated and timely manner.

767 **6.0 GUIDANCE FOR THE DEVELOPMENT OF OPERATIONAL PLANS**

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

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.

773 that will be followed; (2) it contributes to unity of effort by providing a common blueprint for
774 activity in the event of a crisis; and (3) it guides preparedness activities.

775 ***Criteria for Successful Operational Planning***

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

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

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

789 ***Federal Interagency Operational Plan***

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

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

- 796 • Threat overview.
- 797 • Planning assumptions.
 - 798 ○ An imminent terrorist attack in the United States will be the top priority for
799 the U.S.s Government and appropriate Federal departments and agencies will
800 need to respond on short notice.
 - 801 ○ The capabilities of individuals and households, communities and community
802 organizations, private and nonprofit sector, and state and local entities will
803 play a critical role in preventing an imminent terrorist attack.
 - 804 ○ A terrorist attack will occur at any time of day with little or no warning and
805 may involve single or multiple geographic areas.
 - 806 ○ Multiple, near simultaneous terrorist attacks will exceed the capabilities of
807 any one entity.
 - 808 ○ A WMD terrorist attack will result in mass casualties.

- 809 • Concept of operations.
 - 810 ○ Capability modules that detail critical tasks for each capability; supporting and
 - 811 supported responsibilities for each capability; and resource, personnel, and
 - 812 sourcing requirements for each capability.
 - 813 ○ Specific provisions for the rapid integration of resources and personnel
 - 814 through the coordinating structures identified in the Framework.
- 815 • Explanation of how the Federal Interagency Operational Plan for Prevention relates to
- 816 other mission areas, as appropriate.

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

- 819 • Chemical.
- 820 • Biological.
- 821 • Radiological/Nuclear.
- 822 • Explosives/Armed Assault.

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

828 ***State, Local, and Tribal Prevention Planning***

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

836 State and local officials are strongly encouraged to develop a prevention plan in support
837 of the National Prevention Framework. Prevention plans should explain how stakeholders will
838 deliver the Prevention core capabilities and execute the critical tasks outlined in Section 4.0.
839 Additionally, all plans should identify the type of tasks, scope of capabilities, and timeframe of
840 support that each jurisdiction may need from the Federal Government, including any incident
841 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.

842 **7.0 FRAMEWORK MAINTENANCE AND REVIEW CYCLE**

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

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

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

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

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

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

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

¹⁴ PPD-8

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

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