

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

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

This framework is meant to address a number of key issues related to Protection, 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 “**Protection**” 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 PROTECTION FRAMEWORK
FOR NATIONAL REVIEW
20120302, 0800 EST**

1.0 INTRODUCTION

PURPOSE AND DESIRED END STATE

The National Protection Framework provides guidance and unifying principles required to safeguard the Nation against acts of terrorism and man-made or natural disasters. It describes the core capabilities, roles and responsibilities, and coordinating structures that facilitate protection of individuals, communities, and our Nation as a whole. This Framework is focused on actions to protect against the greatest risks to our Nation from all hazards in a manner that allows our interests, aspirations, and way of life to thrive.

Protection is focused on actions to protect the Nation against risks in a manner that allows our interests, aspirations, and way of life to thrive.

Effective protection relies upon close coordination and alignment of the roles and responsibilities of the whole community: individuals; communities; the private sector (business, industry, and nongovernmental organizations); and government at the Federal, state, and local levels as well as with international partners and organizations.^{1,2}

This approach builds on existing plans and processes. It relies on government organizations sharing the responsibility to promote national preparedness through integrated planning while also emphasizing engagement of the whole community within and across the Protection mission area. The National Protection Framework provides the roadmap to promote alignment of Protection efforts and will benefit the whole community by accomplishing the following:

- Providing a unified approach to Protection.
- Enhancing synchronization and interoperability within the Protection mission area and across the Prevention, Mitigation, Response, and Recovery mission areas.
- Fostering collaboration and engagement across the whole community to achieve the objectives of the National Preparedness Goal.

This Framework identifies activities that contribute to protecting the Nation domestically, but it does not address all the capabilities or coordinating structures that may be required to protect U.S. interests overseas.

¹ *Whole community* is defined in the National Preparedness Goal as “a focus on enabling the participation in national preparedness activities of a wider range of players from the private and nonprofit sectors, including nongovernmental organizations and the general public, in conjunction with the participation of Federal, state, and local governmental partners in order to foster better coordination and working relationships.” The National Preparedness Goal is located at <http://www.fema.gov/ppd8>.

² For the purposes of this document, “state and local” includes tribal and territorial governments.

32 **THE NATIONAL PREPAREDNESS GOAL AND THE NATIONAL**
33 **PROTECTION FRAMEWORK**

34 Presidential Policy Directive 8: National Preparedness (PPD-8) establishes five mission
35 areas that combine to ensure the Nation is secure and resilient: Prevention, Protection,
36 Mitigation, Response, and Recovery. It defines Protection as “those capabilities to safeguard the
37 homeland against acts of terrorism and man-made or natural disasters.” Protection mission areas
38 include, but are not limited to, the following: defense against weapons of mass destruction
39 (WMD)³ threats, defense of agriculture and food, critical infrastructure protection, protection of
40 key leadership⁴ and events, border security, maritime security, transportation security,
41 immigration security, cybersecurity, and health security.

42 Implementation of the unified approach in this Framework will achieve the Protection
43 mission area end-state identified in the National Preparedness Goal: to “create conditions for a
44 safer, more secure, and more resilient Nation by enhancing Protection through cooperation and
45 collaboration” with the whole community.

46 **INTENDED AUDIENCE**

47 The Protection Framework provides individual residents; communities; and government,
48 private sector, and nongovernmental organization decision makers with an understanding of the
49 full spectrum of Protection mission activities and what they can do to ensure our Nation is
50 optimally protected from man-made and natural disasters.

51 This Framework is written for and is applicable across government at all levels and the
52 private sector to include: government and corporate executives; law enforcement, security,
53 public health, and emergency management professionals; critical infrastructure owners and
54 operators; and those with legal and/or statutory authorities within the Protection mission area.

55 **2.0 PROTECTION MISSION AREA SCOPE**

56 **PROTECTION MISSION ACTIVITIES**

57 This Framework identifies steady-state and
58 enhanced steady-state mission activities that contribute
59 to protecting the Nation. Protection capabilities⁵
60 include, but are not limited to, the following:

- 61 • **Defense against WMD threats.** Protecting
62 the Nation from threats associated with

Steady-State Activities

Routine, normal, day-to-day operations as contrasted with temporary periods of heightened alert or real-time response to threats or incidents. (Source: *National Infrastructure Protection Plan*)

³ Weapons of mass destruction include chemical, biological, radiological, nuclear, and explosive munitions with the capacity to kill large numbers of human beings indiscriminately.

⁴ Key leaders are defined as current and former Presidents, Vice Presidents, their families, and others granted such protection under Title 18 U.S.C. Sections 3056 and 3056A. Events of national significance fall within two categories: National Special Security Events (NSSEs) and events assessed under the Special Events Assessment Rating (SEAR) process.

⁵ For a more comprehensive explanation of the protection core capabilities, please Section 4.0 of this document.

63 WMD ensures that WMD and related materials and technologies are secure from
64 malicious acquisition, movement, and use within the United States.

65 • **Defense of agriculture and food.** The
66 defense of agriculture and food provides that
67 the Nation’s food and agriculture networks
68 and systems are secured and resilient from
69 all-hazards threats and incidents.

70 • **Critical infrastructure protection.** Critical
71 infrastructure protection activities enhance
72 the safety, security, and resilience of the
73 Nation through protection of the physical,
74 cyber, and human elements of critical
75 infrastructure, including actions to deter the
76 threat, reduce vulnerabilities, and/or
77 minimize the consequences associated with a
78 terrorist attack or other incident.

**Enhanced Steady-State
Activities**

Augmented operations in response to threat information or to support a planned event. An enhanced steady-state condition is caused by a deliberative decision by appropriate leadership to increase capability for a period of time over a particular area. (Sources: *Global Nuclear Detection Architecture Annual Report 201*; *Interagency Domestic Radiological Nuclear Search Operations Plan*)

79 • **Protection of key leadership and events.** The protection of key leadership and
80 events safeguards government executive leadership from hostile acts by terrorists and
81 other malicious actors and ensures security at events of national significance.

82 • **Border security.** Border security activities protect our Nation by securing U.S. air,
83 land, and sea borders against the illegal flow of people and goods while facilitating
84 the flow of lawful travel and commerce.

85 • **Maritime security.** Maritime security activities provide a secure and efficient Marine
86 Transportation System that enables legitimate travelers and goods to move without
87 fear of harm, reduction of civil liberties, or disruption of commerce.

88 • **Transportation security.** Transportation security activities ensure a secure and
89 resilient transportation system, enabling legitimate travelers and goods to move
90 without significant disruption of commerce, undue fear of harm, or loss of civil
91 liberties.

92 • **Immigration security.** Immigration security activities protect the Nation from illegal
93 immigration through effective, efficient immigration systems and processes that
94 respect human rights.

95 • **Cybersecurity.** Cybersecurity activities ensure a safe, secure, and resilient cyber
96 environment that protects privacy and other civil liberties.

97 • **Health security.** Health security activities create a state in which the Nation and its
98 people are prepared for, protected from, and resilient in the face of health threats or
99 incidents with potentially negative health consequences.

100 **GUIDING PRINCIPLES**

101 Three principles guide the development of Protection capabilities to achieve a safer, more
102 secure, and more resilient Nation. These guiding principles are: (1) resilience, scalability, and
103 sustainability; (2) risk-informed culture; and (3) shared responsibility.

- 104 1. **Resilience, Scalability, and Sustainability.** Effective Protection activities minimize
 105 risks from all threats and hazards and strengthen the Nation’s ability to withstand,
 106 respond to, and recover from future incidents.
- 107 a. **Resilience.** Protection activities increase resilience by reducing the impact
 108 and/or duration of disruptive events on organizations and communities.
- 109 b. **Scalability.** Protection plans, programs, policies, and practices are scalable
 110 and flexible to meet unforeseen, unmet, and evolving Protection needs.
- 111 c. **Sustainability.** Protection practices and activities are sustainable to support
 112 the ability of the whole community to meet the needs of the present without
 113 compromising continuing Protection needs. Layered, mutually supporting, and
 114 cyclical capabilities at all levels also allow for sustainment of Protection
 115 capabilities over time.
- 116 2. **Risk-Informed Culture.** A risk-informed culture supports Protection activities. It
 117 relies on vigilance and situational awareness to support information sharing and risk-
 118 informed decisionmaking.
- 119 a. **Vigilance and situational awareness.** Vigilance—being continuously
 120 watchful and aware of threats and hazards—is the first step toward ensuring
 121 the safety and security of our Nation. A comprehensive understanding of
 122 current, evolving, and emerging threats and hazards and the relative risk they
 123 pose forms the strategic foundation of Protection activities.
- 124 b. **Information sharing and risk-informed decisionmaking.** Appropriate,
 125 accessible, and timely information allows for the ongoing analysis of risks and
 126 assessment of best practices. Risk-informed decisionmaking establishes
 127 priorities and helps ensure that investments and operations focus on the most
 128 urgent problems using lessons learned.
- 129 3. **Shared Responsibility.** Protection is most effective as a shared responsibility within
 130 engaged partnerships working together through an integrated process.
- 131 a. **Engaged partnerships.** Partnerships provide a framework to exchange ideas,
 132 approaches, and best practices; facilitate security planning and resource
 133 allocation; establish effective coordinating structures among partners; and
 134 build public awareness. These partnerships allow us to implement Protection
 135 activities consistent with principles of privacy, civil rights, and civil liberties.
 136 Full engagement of public and private partners builds confidence and
 137 ownership of the Protection process among all stakeholders and ensures the
 138 accessibility of information and Protection activities.
- 139 b. **Integrated process.** Working together across all levels of government, both
 140 horizontally and vertically, we can more effectively achieve our shared vision
 141 of a safe and secure Nation that preserves our freedoms and way of life.

142 **RELATIONSHIP WITH OTHER MISSION AREAS**

143 This section describes the relationship between the Protection mission area and the other
 144 mission areas. This includes the identification of shared and discrete core capabilities,
 145 coordinating structures, and roles and responsibilities.

146 The Protection Framework addresses steady-state and enhanced steady-state actions that
147 require coordination for the delivery of core capabilities needed to implement mission activities.
148 These activities continue through all phases and, for the most part, are carried out concurrently
149 with those processes identified in the frameworks for Prevention, Mitigation, Response, and
150 Recovery.

151 Recognizing that Protection efforts may occur simultaneously with other functions,
152 especially Prevention, Mitigation, and Response, the core capabilities and coordinating structures
153 of the Protection Framework can be integrated with those established in the other national
154 frameworks.

155 *Coordination with Prevention Framework*

156 **Prevention** and Protection are closely aligned. The Prevention mission area focuses on
157 intelligence, regulatory, and law enforcement actions that prevent an adversary from attempting
158 to carry out an attack or imminent act of terrorism. Protection activities, on the other hand, focus
159 on decreasing the likelihood of an attack and, like Mitigation, on minimizing the consequences
160 of significant events. While Protection activities may deter an attack, they only do so indirectly.

161 Protection and Prevention share many common elements and rely on many of the same
162 core capabilities. Implementation of Protection and Prevention activities relies on the
163 development and delivery of a common set of core capabilities. Processes described in these
164 frameworks are designed to operate simultaneously in most cases and to provide for seamless
165 transitions when needed to address specific threats. For example, during a period of imminent
166 terrorist threat, Prevention focuses on identification and assessment of threats, determining the
167 impact of the threat, and developing a course of action to prevent the attack. In contrast,
168 Protection assesses the increased risks and coordinates the information sharing and other actions
169 needed to enhance specific protective measures.

170 *Coordination with Mitigation Framework*

171 **Mitigation** refers to longer-term actions taken to reduce loss of life and property by
172 lessening the impact of disasters. Mitigation includes community-wide risk reduction projects,
173 efforts to improve the resilience of specific critical infrastructure lifelines, risk reduction for
174 specific vulnerabilities, and initiatives to reduce future risks after an incident or disaster.

175 Mitigation and Protection mission activities use a risk-informed approach to developing
176 and delivering capabilities. These mission areas share a critical steady-state role. During steady-
177 state conditions, integration of these related and aligned mission areas is achieved through the
178 use of integrated risk information, planning, and coordinating structures. Hazard and risk data
179 will support risk-informed planning, resulting in mitigation strategies that enhance Protection
180 capabilities by reducing risk and vulnerabilities to critical infrastructure and infrastructure
181 sectors. However, some of the most important and effective work is done post-event as
182 additional opportunities and resources, driven by the event, are brought to the table, and as
183 actions are focused on post-event recovery.

184 *Coordination with Response Framework*

185 **Response** includes the capabilities necessary to save lives, protect property and the
186 environment, and meet basic human needs after an incident has occurred. While Protection

187 activities cannot prevent natural disasters from occurring, natural disasters can increase
 188 vulnerabilities that require the implementation of actions developed through the Protection
 189 Framework during response.

190 Efforts to protect people and communities as well as vital facilities, systems, and
 191 resources are inextricably linked to response efforts. Responders support the Protection mission
 192 area and rely on Protection organizations before, during, and after incidents. In the aftermath of
 193 an incident, a secure environment must be established before Response mission area
 194 organizations can deliver essential Response capabilities.

195 Protection resources and capabilities required to support response operations will be
 196 coordinated through the structures identified in the National Response Framework. The
 197 Protection Framework provides the structure to assess and address increased vulnerabilities and
 198 risks beyond the specific disaster area and ensure that protective posture is not compromised.

199 ***Coordination with Recovery Framework***

200 **Recovery** encompasses the capabilities necessary to assist communities affected by an
 201 incident to recover effectively. The systematic evaluation of the threats and hazards affecting the
 202 whole community and the executable strategies derived from that evaluation of the community's
 203 threats and hazards through risk-based planning are foundational to the actions taken during
 204 Recovery. Coordination with the pre- and post-disaster recovery plans will ensure a resilient
 205 Recovery process that takes Protection into account. Protection and Mitigation focus on a
 206 sustainable economy and community resilience and not just the swift restoration of
 207 infrastructure, buildings, and services. Linking Recovery and Protection, Mitigation is an
 208 opportunity for building safer communities.

209 **RISK**

210 Risk is the potential for an unwanted outcome
 211 resulting from an incident, event, or occurrence, as
 212 determined by its likelihood and the associated
 213 consequences. It is assessed based on applicable
 214 threats, vulnerabilities, and consequences.

215 The National Preparedness System is based on
 216 the Strategic National Risk Assessment (SNRA),
 217 which identifies the threats and hazards most likely to
 218 affect the Nation. The core capabilities in the National
 219 Preparedness Goal, in turn, are based on the results of this risk assessment. Planning for and
 220 managing the “greatest risks” is a fundamental component of the National Preparedness Goal
 221 and a compass for all participants who share responsibilities under the National Protection
 222 Framework.

223 Regardless of whether Protection activities occur at the Federal, state, local, or
 224 community level, each entity coordinates with Protection partners vertically and horizontally to
 225 identify, clarify, and prioritize risks. Each entity allocates its individual resources appropriately
 226 to protect against its most likely risks. Collectively, this process prepares the Nation for the
 227 greatest risks.

Risk

The potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences. (Sources: *DHS Risk Lexicon; National Infrastructure Protection Plan*)

228 **RISK MANAGEMENT**

229 Risk management is the process of identifying
 230 and analyzing risk and controlling it to the extent
 231 practicable. The National Protection Framework
 232 contributes to a comprehensive improvement in risk
 233 management by emphasizing the use of risk-informed
 234 decisionmaking for Protection.

235 Risk-informed decisionmaking enables
 236 Protection partners to understand and communicate the
 237 ways in which risk is reduced, accepted, transferred, or
 238 avoided. **Risk reduction** consists of deliberate actions
 239 to reduce the potential for harm from a given risk by
 240 minimizing vulnerabilities, reducing the threat, and/or mitigating consequences (e.g., a business
 241 invests in 24-hour security for better protection). **Risk acceptance** entails a decision not to
 242 change a particular course of action to accommodate an individual risk or component of a risk
 243 (e.g., a business chooses not to invest in 24-hour security because the reduction in risk is
 244 minimal). **Risk transfer** consists of shifting some or all of a particular risk to another entity,
 245 asset, application, system, network, or geographic area (e.g., increasing security at one facility
 246 may make an alternate facility a more attractive target). The last method, **risk avoidance**,
 247 consists of strategies or measures to remove or reduce exposure to a risk (e.g., a community
 248 installs backup power systems for hospitals).

Risk-Informed Decisionmaking
 The determination of a course of action predicated on the assessment of risk, the expected impact of that course of action on that risk, and other relevant factors. Risk-informed decisionmaking includes awareness of and adaptation to changing conditions. (Sources: *DHS Risk Lexicon*; *NIPP*)

249 Sharing risk management information among Protection partners enhances national
 250 preparedness, particularly since risk reduction efforts by one partner may inadvertently increase
 251 another partner’s exposure. Addressing risk both vertically and horizontally fosters a more
 252 holistic approach toward risk management and improves national preparedness.

253 Protection activities are integrated with Mitigation activities to manage risk, as depicted
 254 in Exhibit 1.

255 **Exhibit 1: Integration of Protection and Mitigation for Risk Management**



256
 257 **3.0 ROLES AND RESPONSIBILITIES**

258 Protection partners across the whole community—individuals; the private sector;
 259 academia and research centers; state and local governments; and the Federal Government—are

260 responsible for addressing risk and taking actions to reduce, transfer, accept, or avoid risk within
261 the context of their individual domains. The Protection Framework is designed to provide a
262 cohesive approach to dealing with those risks that can be most effectively reduced, transferred,
263 or avoided through the effective delivery of the Protection mission area activities and core
264 capabilities.

265 **INDIVIDUALS AND THEIR COMMUNITIES**

266 Protection starts at home. Individuals and households provide the foundation for effective
267 protection. By taking actions such as installing and using home security systems or computer
268 protection software, taking first aid or cardiopulmonary resuscitation (CPR) courses, developing
269 a household evacuation plan, reporting suspicious activities, participating in programs such as
270 neighborhood watch, or maintaining an emergency kit at home and at work, individuals can work
271 together to form risk-informed communities.

272 Individuals and communities support the development and delivery of the core capability
273 targets by doing the following:

- 274 • Assisting in the development of critical objectives for community protection plans.
- 275 • Using community reporting mechanisms to report suspicious activities.
- 276 • Taking risk-informed protective measures at home and in communities.

277 Nonprofits and nongovernmental organizations are encouraged to establish or participate
278 in regional and community preparedness partnerships with the whole community so that
279 individuals, employers, businesses, academia, and local government can develop a common
280 understanding of success for their Protection efforts. Where applicable, nonprofits and
281 nongovernmental organizations also contribute to the Protection mission area through the
282 following activities:

- 283 • Protecting assets or information that could be exploited to do harm.
- 284 • Participating in community-based Protection activities.
- 285 • Acting as advocates for, or assistance providers to, a wide range of community
286 members, such as individuals with access and functional needs, children, seniors,
287 individuals with limited English proficiency, and other populations.
- 288 • Helping communities, individuals, and households to receive Protection information
289 and resources.

290 **PRIVATE SECTOR**

291 Private sector organizations own and operate the vast majority of the Nation's businesses
292 and infrastructure. Private sector owners and operators develop and implement the protective
293 programs and resilience strategies for the businesses, infrastructure, and operations under their
294 control. Owners and operators take actions to build Protection capabilities and make investments
295 in security as necessary components of prudent business planning and operations and to ensure
296 continuity of operations. The private sector supports the core capability targets through the
297 following activities:

- 298 • Developing and implementing risk-informed protection plans and measures to ensure
299 resilience and continuity of operations.
- 300 • Coordinating with protection partners to avoid or minimize the impact of threats and
301 hazards on surrounding communities or other industry partners.
- 302 • Protecting physical and cyber assets, networks, applications, and systems that could
303 be exploited to do harm.
- 304 • Ensuring the reliability and integrity of information records and communications
305 systems and services.
- 306 • Maintaining situational awareness of potential threats and hazards in order to support
307 risk-informed decisionmaking.
- 308 • Participating in community preparedness through employee outreach and training
309 programs.
- 310 • Participating in public-private partnerships.

311 **ACADEMIA AND RESEARCH CENTERS**

312 The academic and research center communities play important roles in enabling
313 protection efforts and implementation at all levels of government by doing the following:

- 314 • Conducting research to identify new protection technologies.
- 315 • Researching and providing innovative perspectives on threat protection.
- 316 • Preparing or disseminating protection guidelines, courses, and descriptions.
- 317 • Developing suitable all-hazards protection courses.
- 318 • Establishing protection-related curricula and degree programs.

319 Protection activities by academia and research centers include risk assessment,
320 development of plans, training/exercising, and taking other concrete steps to protect their
321 facilities, technology, personnel, and sensitive/dual-use materials from being compromised.

322 **LOCAL GOVERNMENT**

323 Local governments generally represent the front lines for homeland security and
324 community and infrastructure protection. Local governments support accomplishment of the core
325 capability targets by doing the following:

- 326 • Developing and delivering the core capabilities needed for local and community
327 protection.
- 328 • Acting as a focal point for and promoting the coordination of Protection activities,
329 preparedness programs, and resource support within the community.
- 330 • Participating in national, state, local, and regional education and awareness programs.
- 331 • Participating in the exchange of security information—including threat assessments,
332 attack indications and warnings, and advisories—among partners.

- 333 • Sharing with partners information deemed to be critical from the local perspective to
334 enable prioritized protection of critical public services, facilities, utilities, and
335 processes.
- 336 • Coordinating with private sector entities, infrastructure owners and operators, and
337 jurisdictions to protect public health, safety, and security while ensuring the free flow
338 of commerce and preservation of civil liberties.
- 339 • Conducting investigations and engaging in enforcement and protective actions based
340 on jurisdictional authorities.
- 341 • Identifying, implementing, and monitoring a risk management plan.
- 342 • Ensuring that funding priorities are addressed and that protection resources are
343 allocated.
- 344 • Implementing measures to identify critical infrastructure, determine risk, train and
345 exercise, and take corrective measures.
- 346 • Establishing continuity plans and programs.
- 347 • Addressing unique geographical protection issues, including transborder concerns,
348 dependencies, and interdependencies among agencies and enterprises.
- 349 • Entering into mutual aid agreements with neighboring communities.

350 **STATE GOVERNMENTS**

351 State governments are responsible for the public safety, security, public health, and
352 welfare of the people in their jurisdictions. State governments are responsible for the following:

- 353 • Developing and delivering the core capabilities needed for Protection activities within
354 their jurisdictions.
- 355 • Serving as crucial coordination hubs, bringing together Protection authorities,
356 capabilities, and resources among local jurisdictions, across sectors, and between
357 regional entities.
- 358 • Coordinating with private sector entities, infrastructure owners and operators, and
359 jurisdictions to protect public health, safety, and security while ensuring the free flow
360 of commerce, the protection of civil rights, and the preservation of civil liberties.
- 361 • Conducting investigations and engaging in enforcement and protective actions based
362 on jurisdictional authorities.
- 363 • Establishing partnerships, facilitating coordinated information sharing, and enabling
364 planning and protection of critical infrastructure within their jurisdictions.
- 365 • Addressing unique geographical Protection issues, including transborder concerns,
366 dependencies, and interdependencies among agencies and enterprises.
- 367 • Establishing agreements and ensuring readiness for cross-jurisdictional coordination.

368 As sovereign nations, tribal governments govern and manage the safety and security of
369 their lands and community members along with their Federal partners. Many tribal government

370 borders cross multiple counties and states, presenting a unique challenge in planning and
 371 coordinating Protection efforts. Federal, state, and local governments work with the sovereign
 372 tribal governments to ensure integration of their protection plans.

373 The integration of statewide and regional Protection efforts into the existing homeland
 374 security programs ensures that Prevention, Protection, Mitigation, Response, and Recovery
 375 efforts are synchronized and mutually supportive.

376 **FEDERAL GOVERNMENT**

377 The Federal Government provides a leadership, coordination, and integration role in the
 378 development and delivery of Protection capabilities. Federal departments and agencies
 379 implement statutory and regulatory responsibilities for a wide array of protective programs and
 380 provide assistance in a number of areas, including funding, research, coordination, oversight, and
 381 implementation.

382 The Federal Government, in coordination with state and local partners, contributes to
 383 achieving the goals of the Protection mission area by doing the following:

- 384 • Identifying the core capabilities needed for Protection activities.
- 385 • Establishing mechanisms and providing the full spectrum of support necessary for
 386 appropriate information sharing among all levels of government, the private sector,
 387 and nongovernmental organizations.
- 388 • Monitoring, detecting, and analyzing threats to public health, safety, and security.
- 389 • Conducting vulnerability assessments, performing risk analyses, and coordinating
 390 protective measures in conjunction with the private sector and Federal, state, and
 391 local organizations and agencies.
- 392 • Providing expertise and coordination for Protection planning efforts and conducting
 393 technical assessments (e.g., vulnerability assessments, risk analyses, and surveillance
 394 sensor architecture).
- 395 • Establishing and implementing national laws, regulations, guidelines, and standards
 396 designed to protect public health, safety, and security while ensuring the free flow of
 397 commerce, the protection of civil rights, and the preservation of civil liberties.
- 398 • Coordinating with private sector entities, infrastructure owners and operators, and
 399 jurisdictions to protect public health, behavioral health, safety, and security while
 400 ensuring the free flow of commerce, the protection of civil rights, and the
 401 preservation of civil liberties.
- 402 • Coordinating and collaborating with international partners and organizations to
 403 promote risk-based principles and coordinated protective efforts.
- 404 • Conducting investigations and engaging in enforcement and protective actions based
 405 on agency authorities.
- 406 • Providing integrated Federal public safety and security capabilities and resources for
 407 potential or actual incidents requiring a coordinated Federal response.

- 408 • Implementing grant programs for Protection activities at the state, local, and private
409 sector levels, as authorized by Congress.

410 The Department of Defense (DOD) conducts homeland defense and civil support
411 missions to deter war and protect U.S. territory, persons, and infrastructure from attack. DOD
412 routinely conducts Protection activities such as cybersecurity, maritime security, transportation
413 security, and other missions outside of, and in anticipation of, activities within the National
414 Protection Framework. DOD leads the homeland defense mission to protect U.S. sovereignty,
415 territory, the domestic population, and the defense industrial base against external threats and
416 aggression or other threats as directed by the President. DOD also provides defense support to
417 civil authorities for domestic incidents as directed by the President or when consistent with
418 military readiness and appropriate under the circumstances and the law. At the request of the
419 Secretary of Homeland Security, DOD support may include, but is not limited to, monitoring and
420 interdicting WMD materials at borders, ports of entry, and other locations within the United
421 States. At the request of the Attorney General, DOD support to law enforcement may include,
422 but is not limited to, incident awareness and assessment, search and detection, interdiction and
423 disruption, forensics and attribution, planning, and transportation and logistics support.

424 **AUTHORITIES**

425 The authority for the Protection mission is established in Federal, state, and local laws,
426 regulations, ordinances, and other directives with the force and effect of law. This Framework
427 does not change or replace any existing authorities.

428 Federal departments and agencies have differing authorities regarding Protection. Exhibit
429 7 provides a list of primary coordinating agencies that have responsibility for the specified
430 mission activities.

431 Within and across several critical infrastructure sectors, Federal statute, Executive
432 Orders, and regulations empower a number of Federal agencies to oversee and assist in aspects
433 of the protection of the sector members. Notwithstanding other provisions of this Framework, the
434 planning and execution of Framework activities will assure deconfliction with the authorities and
435 responsibilities of those agencies and their requirements within the respective sector. This
436 applies to planning and execution at all levels in those sectors within the agencies’
437 responsibilities. Organizations having responsibility for such planning and execution will
438 incorporate consultation and coordination with those agencies into their actions to assure
439 appropriateness and compatibility and consideration of the agencies’ work as an aspect of sector
440 protection.

441 **4.0 PROTECTION CORE CAPABILITIES**

442 The National Preparedness Goal identified the core capabilities⁶ needed for each of the
443 five mission areas—Prevention, Protection, Mitigation, Response, and Recovery (see Exhibit 2).
444 The approach to developing and delivering these core capabilities will differ according to and
445 across the mission areas.

⁶ The core capabilities represent an evolution from the Target Capabilities List. The transition to core capabilities expands the focus to include Mitigation and allows greater focus on Prevention and Protection activities based on experience since the release of Homeland Security Presidential Directive 8 (HSPD-8).

446 The Protection mission area identifies 11 core capabilities, three of which—planning,
447 public information and warning, and operational coordination—crosscut all of the mission areas.
448 In addition, the Protection and Prevention mission areas share three core capabilities: intelligence
449 and information sharing; interdiction and disruption; and screening, search, and detection.

450 There also are linkages between Protection, Mitigation, Response, and Recovery through
451 the remaining capabilities, such as threat and hazard identification, risk and disaster resilience
452 assessment, and infrastructure systems recovery.

453 **COMMON CORE CAPABILITIES**

454 The following three core capabilities span all five mission areas:

- 455 • **Planning.** Protection planning is a systematic process that engages the whole
456 community, as appropriate, in the development of executable strategic, operational, or
457 community-based approaches to meet defined Protection objectives.
- 458 • **Public Information and Warning.** Engaging the whole community in Protection
459 requires the delivery of coordinated, prompt, reliable, and actionable information to
460 the whole community through the use of clear, consistent, accessible, and culturally
461 and linguistically appropriate methods. These efforts will be implemented to
462 effectively relay information regarding any imminent threat and, as appropriate, the
463 actions being taken and the assistance being made available.
- 464 • **Operational Coordination.** Unified and coordinated operational structures and
465 processes allow for the integrated delivery of Protection capabilities across
466 stakeholders and mission areas.

467

Exhibit 2: Core Capabilities by Mission Area (Source: National Preparedness Goal)

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

468

PROTECTION CORE CAPABILITIES

469

The remaining Protection core capabilities are the following:

470

- **Intelligence and Information Sharing.** All actions within the Protection Framework begin with the monitoring, gathering, and analysis of intelligence and information.

471

472

- Intelligence is the provision of timely, accurate, and actionable information to the appropriate jurisdiction concerning actual or perceived threats against the United States or any other matter bearing on U.S. national or homeland security.

473

474

475

- 476 ○ Information sharing is the ability to exchange intelligence, information, data,
477 or knowledge among Federal, state, and local governments; private sector
478 entities; and international partners, as appropriate.
- 479 ● **Interdiction and Disruption.** Integrated Prevention and Protection capabilities work
480 to delay, divert, intercept, halt, apprehend, or secure people, materials, or activities
481 that pose a threat to the Nation.
- 482 ● **Screening, Search, and Detection.** Prevention and Protection mission areas rely on
483 the application of active and passive surveillance and search procedures to identify,
484 discover, or locate threats or hazards. These may include the use of systematic
485 examinations and assessments, sensor technologies, disease surveillance, laboratory
486 testing, or physical investigation and intelligence.
- 487 ● **Access Control and Identity Verification.** The application of a broad range of
488 physical, technological, and cyber measures provides Protection by controlling and
489 limiting access to critical locations and systems to authorized individuals carrying out
490 legitimate activities.
- 491 ● **Cybersecurity.** A key component of Protection involves securing and, if needed,
492 restoring electronic communications systems and services and the information
493 contained therein against or from damage, unauthorized use, or malicious
494 exploitation.
- 495 ● **Physical Protective Measures.** Protection is enhanced by the implementation of
496 physical measures to reduce risks by controlling movement and protecting borders,
497 critical infrastructure, and the homeland.
- 498 ● **Risk Management for Protection Programs and Activities.** The identification,
499 assessment, and prioritization of risks form the basis for all Protection activities and
500 investments.
- 501 ● **Supply Chain Integrity and Security.** The protection of supply chain integrity relies
502 on the application of measures designed to strengthen its security and resilience.

503 **CRITICAL PROTECTION CAPABILITY OBJECTIVES**

504 Collectively, the core capabilities for the Protection mission area provide the foundation
505 for achieving the overarching critical objective for Protection: a homeland that is protected from
506 terrorism and other hazards, and in which American interests, aspirations, and the American way
507 of life can thrive.

508 The National Preparedness Goal established target objectives for each of the Protection
509 mission core capabilities. These targets or critical objectives, as contained in the National
510 Preparedness Goal, are listed in Exhibit 3. The critical objectives are specific to Protection and
511 can be used by jurisdictions at all levels and by other Protection partners to identify tailored
512 goals and objectives using the steady-state Protection process described in this Framework.

513 The critical objectives associated with the Protection core capabilities are ambitious.
514 They are not targets for any single jurisdiction or agency; rather, achieving these objectives will
515 require a national effort involving the whole community.

Exhibit 3: Critical Protection Capability Objectives

Row	Core Capability	Critical Objectives
1	Planning	<ol style="list-style-type: none"> 1. Develop protection plans that identify critical objectives based on planning requirements, provide a complete and integrated picture of the sequence and scope of the tasks to achieve the planning objectives, and implement planning requirements within the timeframe contemplated within the plan using available resources for protection-related plans. 2. Implement, exercise, and maintain plans to ensure continuity of operations.
2	Public Information and Warning	Use effective and accessible indication and warning systems to communicate significant hazards to involved operators, security officials, and the public (including alerts, detection capabilities, and other necessary and appropriate assets).
3	Operational Coordination	Establish and maintain partnership structures among Protection elements to support networking, planning, and coordination.
4 The capabilities below are necessary to both the Prevention and Protection mission areas. Plans and activities should be integrated across the two mission areas.		
5	Intelligence and Information Sharing	<ol style="list-style-type: none"> 1. Anticipate and identify emerging and/or imminent threats through the intelligence cycle. 2. Share relevant, timely, accessible, and actionable information and analysis with Federal, state, local, private sector, and international partners and develop and disseminate appropriate classified/unclassified products. 3. Provide Federal, state, local, and private sector partners with or access to a mechanism to submit terrorism-related information and/or suspicious activity reports to law enforcement.
6	Interdiction and Disruption	<ol style="list-style-type: none"> 1. Deter, detect, interdict, and protect against domestic and transnational criminal and terrorist activities that threaten the security of the homeland across key operational activities and critical infrastructure sectors. 2. Intercept the malicious movement and acquisition/transfer of chemical, biological, radiological, nuclear, and explosive (CBRNE) materials and related technologies.
7	Screening, Search, and Detection	<ol style="list-style-type: none"> 1. Screen cargo, conveyances, mail, baggage, and people using information-based and physical screening technology and processes. 2. Detect WMD, traditional, and emerging threats and hazards of concern using: <ol style="list-style-type: none"> a. A laboratory diagnostic capability and the capacity for food, agricultural (plant/animal), environmental, medical products, and clinical samples. b. Bio-surveillance systems. c. CBRNE detection systems. d. Trained healthcare, emergency medical, veterinary, and environmental laboratory professionals.

Row	Core Capability	Critical Objectives
8	The capabilities below are unique to the Protection mission area; however there are linkages to other mission area capabilities. Plans and activities should be integrated as necessary.	
9	Access Control and Identity Verification	Implement and maintain protocols to verify identity and authorize, grant, or deny physical and cyber access to specific locations, information, and networks.
10	Cybersecurity	<ol style="list-style-type: none"> 1. Implement risk-informed guidelines, regulations, and standards to ensure the security, reliability, integrity, and availability of critical information, records, and communications systems and services through collaborative cybersecurity initiatives and efforts. 2. Implement and maintain procedures to detect malicious activity and to conduct technical and investigative-based countermeasures, mitigations, and operations against malicious actors to counter existing and emerging cyber-based threats, consistent with established protocols.
11	Physical Protective Measures	Implement and maintain risk-informed physical protections, countermeasures, and policies protecting people, structures, materials, products, and systems associated with key operational activities and critical infrastructure sectors.
12	Risk Management for Protection Programs and Activities	<ol style="list-style-type: none"> 1. Ensure critical infrastructure sectors and protection elements have and maintain risk assessment processes to identify and prioritize assets, systems, networks, and functions. 2. Ensure operational activities and critical infrastructure sectors have and maintain appropriate threat, vulnerability, and consequence tools to identify and assess threats, vulnerabilities, and consequences.
13	Supply Chain Security and Integrity	Secure and make resilient key nodes, methods of transport between nodes, and materials in transit.

517 **5.0 COORDINATING STRUCTURES AND INTEGRATION**

518 As described in PPD-8, the National Protection Framework is intended to identify
 519 scalable, flexible, and adaptable coordinating structures to align the key roles and responsibilities
 520 to deliver the core capabilities for the mission areas. The Protection Framework promotes
 521 integration of existing coordinating structures at all levels of government to enable the effective
 522 delivery of the Protection core capabilities.

523 **COORDINATING STRUCTURES**

524 Coordinating structures provide the mechanisms to develop and deliver core capabilities
 525 at all levels of government and the private sector across the full range of Protection mission
 526 activities. This Framework recognizes, values, and leverages the robust array of existing
 527 coordinating structures, and identifies a Protection cycle and guiding principles that promote
 528 integration and synchronization across the various jurisdictions and areas of responsibility.

529 These coordinating structures both support steady-state Protection program
 530 implementation and strengthen the Nation’s ability to increase the protective posture and
 531 enhanced steady-state Protection resources during periods of heightened alert, terrorist threats, or
 532 times of increased vulnerability due to impending or actual disasters. These structures exist to

533 conduct planning, implement training and exercise programs, promote information sharing,
 534 address common vulnerabilities, align resources, and promote the delivery of Protection
 535 capabilities.

536 Coordinating structures identified for this Framework are organized to enhance the
 537 effectiveness of the specified mission activities.

538 The range of coordinating structures that contribute to the Protection mission area
 539 includes, but is not limited to, the following: operations centers, state and major urban area
 540 fusion centers, government councils, coordinating councils and governance boards, regional
 541 consortiums, information-sharing mechanisms, public health surveillance networks, and public-
 542 private partnership organizations at all levels.

543 **COMMUNITY, STATE, AND REGIONAL COORDINATING STRUCTURES**

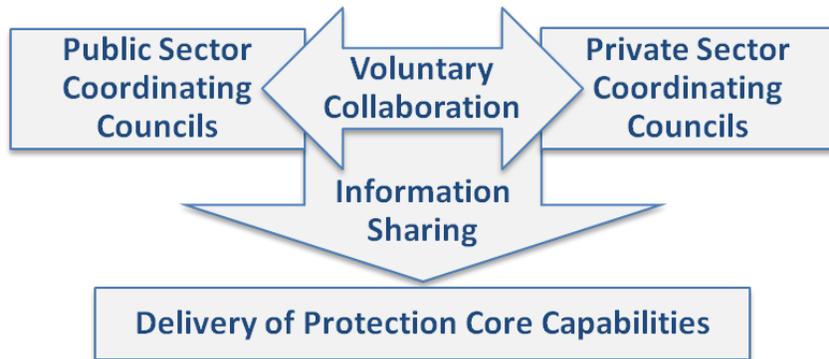
544 *Coordination through Partnerships*

545 Protection capabilities are coordinated through existing partnerships at all levels of
 546 government and with the private sector and nongovernmental organizations. There are numerous
 547 examples of existing Protection partnerships ranging from neighborhood watch programs to
 548 regional government councils, joint task forces, and infrastructure protection sector coordinating
 549 councils. Many community and regional coordination groups and councils that have been
 550 established are designed to promote a higher level of understanding about Protection and
 551 Preparedness and to cross sector and geographical boundaries. These partnerships allow for the
 552 exchange of expertise and information and provide a source of potential resources through
 553 mutual aid and assistance agreements. This Framework promotes the continued use of a
 554 partnership model to coordinate the delivery of Protection capabilities and enhance whole
 555 community preparedness.

556 Because of the specific challenges and interdependencies facing individual regions and
 557 the broad range and diversity of public- and private sector Protection partners, regional efforts
 558 are often complex. The Regional Consortium Coordinating Council (RCCC) enables Protection
 559 coordination among partners within and across geographic areas and sectors.

560 As illustrated in Exhibit 4 below, partnership councils at all levels enable the voluntary
 561 public-private collaboration essential to sustaining Protection programs and the delivery of core
 562 capabilities for the Protection mission activities.

563 **Exhibit 4: Partnership Councils and Delivery of Protection Core Capabilities**



564

565 ***Operational Coordination***

566 In most jurisdictions, local operations centers are the focal point for coordinating the
567 delivery of Protection capabilities to the whole community. In addition, state and major urban
568 fusion centers serve as focal points within the state and local environments for the receipt,
569 analysis, gathering, and sharing of threat-related information between government and private
570 sector partners, while Joint Terrorism Task Forces (JTTFs) focus on terrorism-related
571 investigations.

572 ***Coordination through Established Systems***

573 This Framework promotes the use of principles such as those contained in the National
574 Incident Management System (NIMS) to coordinate Protection activities across all levels of
575 government, the private sector, and nongovernmental organizations. These systems provide
576 guidelines to enable organizations with different legal, geographic, and functional
577 responsibilities to coordinate, plan, and interact effectively. Each participating organization
578 maintains its authority, responsibility, and accountability.

579 **NATIONAL-LEVEL COORDINATING STRUCTURES**

580 At the national level, an array of coordinating structures exists to facilitate partnerships,
581 planning, information sharing, and resource and operational synchronization across all aspects of
582 the Protection mission area. These structures include, but are not limited to, the following:
583 operations and information centers; public-private partnerships, councils, and boards; and other
584 entities that are established to address specific mission activities and promote a unified approach
585 to Protection. This section focuses on the policy-level coordination conducted through White
586 House leadership, public-private partnerships, and those structures that are in place or need to be
587 established to ensure a coordinated approach to Protection across the whole community.

588 ***National Security Council***

589 The President leads the Federal Government Protection effort to ensure that the necessary
590 coordinating structures, leadership, and resources are applied quickly and efficiently to deliver
591 the Protection core capabilities. The President’s National Security Council, which brings
592 together Cabinet officers and other department or agency heads as necessary, provides national
593 strategic and policy advice to the President during large-scale incidents that affect the Nation.

594 ***Transborder Security Interagency Policy Committee***

595 The Transborder Security Interagency Policy Committee (IPC) provides policy
596 coordination, dispute resolution, and periodic in-progress reviews for the development of
597 national-level performance objectives to achieve the National Preparedness Goal’s core
598 capabilities for Protection, as well as for the development of the National Protection Framework.

599 ***Federal Departments and Agencies***

600 In accordance with PPD-8, “The Secretary of Homeland Security is responsible for
601 coordinating the domestic, all-hazards preparedness efforts of all executive departments and
602 agencies, in consultation with State, local, tribal, and territorial governments, nongovernmental
603 organizations, private sector partners, and the general public.” Further, the PPD-8
604 Implementation Plan assigns specific responsibilities to the Secretary of Homeland Security that

605 include coordinating “the development and implementation of capabilities related to protection
606 (except for defense activities which are the responsibility of the Secretary of Defense), and the
607 development of the National Protection Framework and associated interagency operations
608 plans.”

609 The Federal Government promotes coordination within and across the Protection mission
610 area through a wide range of coordinating structures that include, but are not limited to, the
611 following: headquarters-level operations and information centers; coordinating councils and
612 information-sharing mechanisms; and boards, working groups, and task forces formed to address
613 specific Protection mission activities, requirements, or threats.

614 Under the Protection Framework, various Federal departments or agencies assume
615 primary coordinating roles based on their authorities, the specific mission activities, and the
616 nature of the threat or hazard (refer to Exhibit 7). These Federal departments and agencies
617 provide the basis for the ongoing coordination and collaboration that will be required to promote
618 implementation and ensure the ongoing management and maintenance of the Protection
619 Framework and other Protection preparedness requirements established through PPD-8.

620 *National-Level Partnership Councils*

621 For many of these mission activities—defense of agriculture and food, critical
622 infrastructure protection, maritime security, transportation security, cybersecurity, and health
623 security—the established sector, government, and coordination councils and information-sharing
624 mechanisms such as Information Sharing and Analysis Centers (ISACs) provide the foundation
625 for Protection planning, risk management, and the implementation of protective programs.

626 The National Infrastructure Protection Plan (NIPP), for example, promotes the use of a
627 sector partnership model as the primary organizational structure for coordinating infrastructure
628 protection efforts and activities. Sector-Specific Agencies (SSAs), as identified in Homeland
629 Security Presidential Directive 7 (HSPD-7), Critical Infrastructure Identification, Prioritization,
630 and Protection, are responsible for critical infrastructure protection activities in specified sectors.
631 Each sector has built partnerships with sector stakeholders, including facility owners and
632 operators; Federal, state, and local government agencies; the law enforcement community; trade
633 associations; and state homeland security advisors. SSAs are responsible for working with both
634 public and private partners to develop protective programs and resilience strategies.

635 The sector partnership model encourages formation of Sector Coordinating Councils
636 (SCCs) and Government Coordinating Councils (GCCs). Together, SCCs and corresponding
637 GCCs create a coordinated national structure for infrastructure protection within and across
638 sectors. Additional information on the coordinating councils can be found in the NIPP.

639 *Interagency Protection Coordination Group*

640 Coordination across all of the Protection mission activities will be achieved through an
641 Interagency Protection Coordination Group (IPCG) comprised of representatives from those
642 Federal departments and agencies with statutory and or/regulatory authority pertinent to the
643 Protection mission. This group fills the need for coordination across all Protection mission
644 activities and core capabilities. The IPCG will do the following:

- 645 • Promote Protection preparedness and coordination to ensure the development and
646 delivery of Protection core capabilities across the mission activities.

- 647 • Provide the mechanisms for steady-state integration with Prevention, Mitigation,
648 Response, and Recovery and promote Protection collaboration across the whole
649 community.
- 650 • Meet periodically (at least twice annually) to ensure the ongoing management and
651 maintenance of the Protection Framework, guide efforts for interagency Protection
652 planning, address common concerns, and take other actions as required.

653 **STEADY-STATE PROTECTION PROCESS**

654 This section summarizes the process to identify the measures necessary to protect against
655 threats and hazards under steady-state conditions, i.e., within an organization’s charter or
656 mission, conducted on a routine basis (e.g., day-to-day), and within an anticipated level of effort.
657 The responsibility for steady-state protection is shared by all levels of government and the
658 private sector. Protection actions take place primarily at the community and facility levels.

659 Protection actions are taken at the borders and along the coastline, at international points
660 of entry, at major transportation hubs, and across every critical infrastructure sector.

661 All entities that are responsible for Protection—including governments at all levels,
662 critical infrastructure owners and operators, and businesses—are encouraged to use the steady-
663 state coordinating process to identify Protection core capabilities and determine how those
664 capabilities will be delivered.

665 Exhibit 5 depicts the steady-state Protection process, described below.
666

Exhibit 5: Steady-State Protection Process



667

- 668
669
670
671
672
673
674
675
676
677
1. **Identify Protection mission goals and objectives.** The first step of the process is to identify the Protection mission for the community or jurisdiction. Desired goals and objectives may vary across and within jurisdictions or areas of responsibility, depending on the risk landscape and operating environment. Goals and objectives that are collaboratively derived help establish a common vision of the desired long-term security posture and recovery criteria and should reflect the broad Protection and Recovery goals of the full range of partners. Protection partners also can draw on these goals during risk management to best determine which specific Protection core capabilities and risk-reduction and protective strategies most significantly enhance security in the area.

678
679
680
681
682
683
684
685
686
687
688

 2. **Engage coordination partners.** This step of the Protection cycle determines the size and scope of the community's/jurisdiction's local coordinating structures by identifying key stakeholders. These stakeholders (Protection partners) will identify the Protection core capabilities needed based on the Protection mission and how the core capabilities will be delivered. Potential partners include the following: critical infrastructure and business owners and operators; government organizations (Federal, state, local, and regional entities); community associations and other organizations; professional, trade, and business associations; advisory councils; academia and research centers; nongovernmental organizations; and international partners. During engagement, the roles and responsibilities for each Protection partner should be delineated.

689
690
691
692
693
694
695
696
697

 3. **Gather data.** Data gathering identifies issues associated with identifying goals and objectives and identifying the size and scope of coordinating structures. During this step, the community gathers data concerning potential threats and hazards from international and domestic terrorism, other human-caused incidents, natural disasters, and infrastructure failures. Data gathering identifies potential issues, challenges, or vulnerabilities that may be associated with the specific activity or the size and scope of the mission. Historical information is useful in predicting the possible scope of future events and likelihood of reoccurrence. This information will be used to perform a risk assessment for the community.

698
699
700
701

 4. **Assess and analyze risk.** During this step, the community assesses and analyzes risks. A specific methodology for the risk assessment is not prescribed. Whatever the method used, it is important to assess all potential threats, hazards, and vulnerabilities.

702
703
704

 5. **Evaluate and prioritize.** In this step, communities evaluate potential risks and prioritize Protection efforts based on the Protection mission and goals developed earlier in the process.

705
706
707
708
709
710
711

 6. **Implement protective activities.** In the final step, communities identify the core capabilities and elements needed to achieve Protection. Protection activities can include a range of activities, including the sharing of effective practices, implementing public information and warning processes and mechanisms, and training and exercising together. This step includes actions to ensure continuous improvement, such as training and exercising and evaluating the effectiveness of Protection activities and programs. The gathering of lessons learned and evaluation

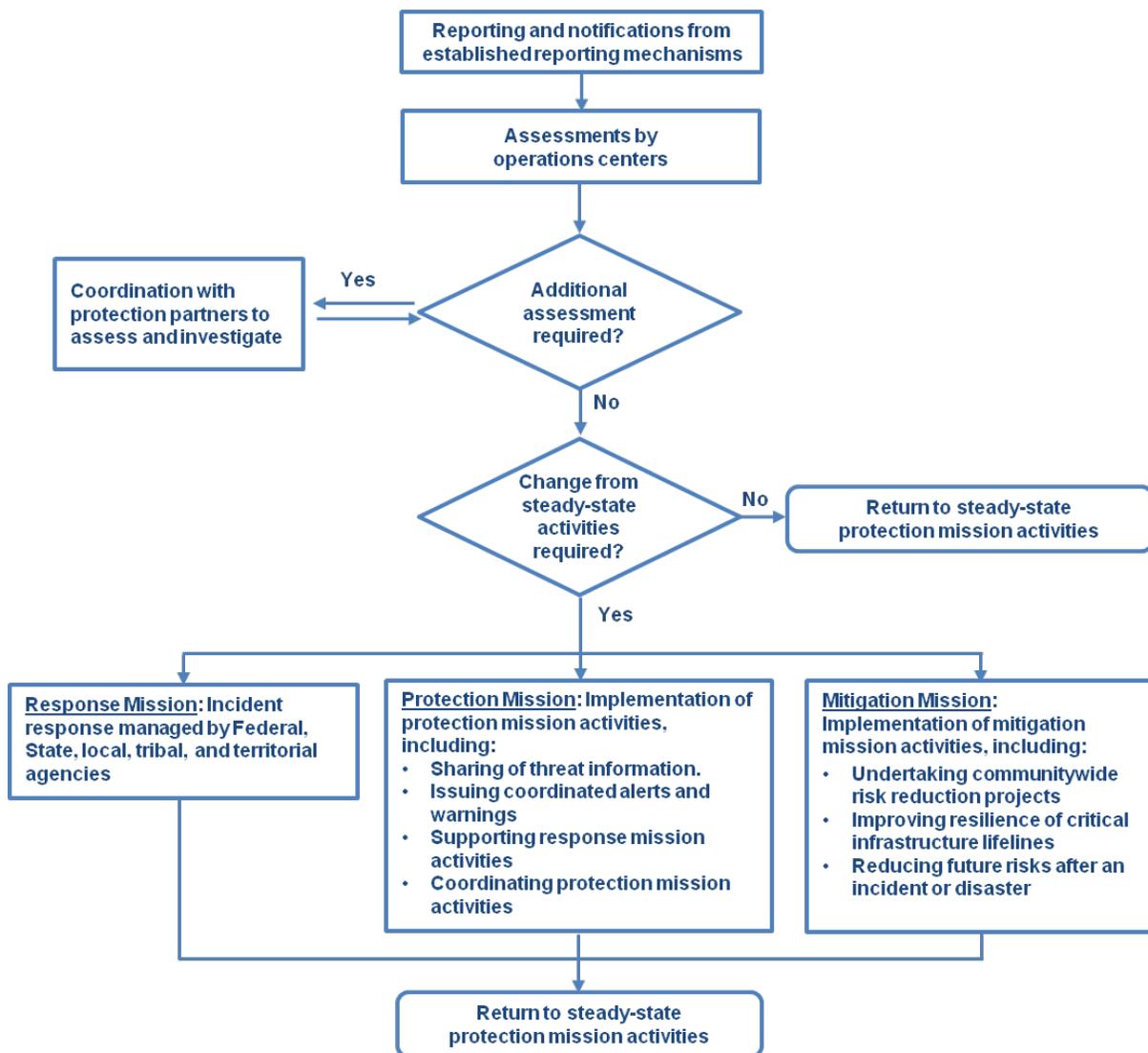
712 results may lead the community or jurisdiction to revisit any of the steps in the
 713 process.

714 **PRE-INCIDENT COORDINATION PROCESS**

715 Assessment and pre-incident interagency coordination may be compressed during periods
 716 of elevated threat or impending disasters. In this instance, communities move quickly to
 717 coordinate multiple jurisdictional Protection activities—e.g., information-sharing, interagency
 718 course of action development, communications planning/coordination, alert and deployment of
 719 resources, and other assistance as required—in consultation and coordination with Federal
 720 departments and agencies and the affected jurisdiction(s). Exhibit 6 depicts this pre-incident
 721 coordination process.

722

Exhibit 6: Pre-Incident Coordination Process



723

- 724 • **Reporting and Notifications.** Federal, state, local, private sector, and
 725 nongovernmental organizations share information about potential threats and hazards
 726 using established communications and reporting channels. Depending on the type of

727 threat or hazard, Federal, state, and local organizations either are required or
 728 encouraged to report the potential threat and hazard information following existing
 729 mechanisms and legal requirements. Private sector and nongovernmental
 730 organizations are encouraged to use existing jurisdictional threat-reporting
 731 mechanisms.

732 • **Assessments.** Governments at all levels maintain operational watch and response
 733 centers to maintain situational awareness by monitoring all levels and types of
 734 potential threats to safety and security. If needed, operations centers coordinate with
 735 additional Protection partners to further assess and investigate potential threats.

736 • **Response and Enhanced Steady-state Protection Activities.** Following assessment
 737 of the situation, the situation may require the initiation of Response mission activities
 738 and a change from Protection steady-state to enhanced steady-state activities.
 739 Examples of enhanced steady-state Protection mission activities may include the
 740 following:

741 ○ Sharing of threat information including the issuances of watches, warnings,
 742 and other emergency bulletins. For example, the National Weather Service
 743 issues weather-related notices to warn the public of impending storms and
 744 severe weather. A number of surveillance systems are used routinely by public
 745 health departments at the national, state, and local levels to monitor public
 746 health risks.

747 ○ Supporting Response mission activities by making sure that communities and
 748 responders have adequate protection during the crisis.

749 ○ Coordinating Protection mission activities through implementation of
 750 Protection authorities and provision of resources.

751 • **Return to Steady-state Protection Activities.** When enhanced steady-state
 752 Protection actions are no longer needed, there is a return to steady-state Protection
 753 mission activities.

754 **INTEGRATION**

755 There is a need to address integration at all levels of government and within each of the
 756 five preparedness mission areas to ensure synchronization and interoperability. Integration
 757 occurs through the following activities:

- 758 • Addressing risk.
- 759 • Planning and exercising coordination and communication procedures.
- 760 • Sharing resources.

761 Organizations and individuals involved in the Protection mission area work together to
 762 determine how to address risk, plan and exercise coordination and communication procedures,
 763 and share resources. Successful Protection activities require synchronization and interoperability
 764 among partners, communities, and mission areas as appropriate. These three integrating factors
 765 help to align Protection plans and activities, make them mutually supportive, and maximize
 766 efficiencies across all levels of government and the whole community.

767 Examples and more details about each of the integrating factors are provided below.

768 ***Addressing Risk***

769 The following is an example of risk as an integrating factor:

770 If an organization in the Protection mission area identifies earthquakes as a risk, it should
771 coordinate with the appropriate partners across mission areas to exchange information
772 and expertise. This process could identify potential new vulnerabilities that are created as
773 Protection resources are deployed to support the disaster response and recovery.

774 The results of this coordination will inform all involved mission areas and can be useful
775 in many ways, such as building consistency and integrating efforts. Working across mission
776 areas enables Protection organizations to work with planners who are actively involved in
777 earthquake planning, share modeling and scenarios, and integrate courses of action. Most
778 importantly, the organizations from the various mission areas work in concert to address the
779 same risk.

780 ***Planning and Exercising Coordination and Communication Procedures***

781 Protection entities need to understand how they will coordinate Protection activities with
782 one another. Planning and exercising those plans together allows all Protection partners to align
783 and support one another to ensure unity of effort.

784 Coordination and communications represent an important integrating factor for two
785 reasons. First, coordination and communication structures vary among mission areas. A mutual
786 understanding of these structures across all mission areas enables planners to develop procedures
787 to deal with these differences so mission areas can operate together cohesively.

788 Second, organizations in each mission area have their own authorities, policies, and
789 strategies for delivering protection capabilities. Analysis of the structures across all mission areas
790 (and vertically and horizontally) often reveals competing authorities, interdependencies,
791 overlaps, and gaps. Understanding and documenting these relationships is key to effective
792 operational planning.

793 ***Resource Sharing***

794 While as a Nation we are committed to making use of whatever resources are available to
795 ensure preparedness, we acknowledge that available resources are finite. A holistic perspective
796 about resources helps to ensure that some resources are not over-assigned while others remain
797 underutilized. To overcome this issue, Protection entities must coordinate across the whole
798 community to ensure that required resources are and will be available when needed, particularly
799 if those resources can be used to avert a threat or hazard. Approaching resources holistically in
800 identifying Protection activities aids in the development of innovative resourcing solutions.

801 Estimates of what resources are needed and what resources are available—indicating
802 where there are gaps and where extra resources are available—can be coordinated with
803 appropriate Protection partners both vertically and horizontally as a key step during the
804 Protection process.

805 Guidance for this integrating factor includes the following:

- 806 • Protection partners need to consider resources from the whole community to
807 maximize unity of effort and effectiveness, and reduce costs and time of delivery.
808 Emphasis should be placed on innovative and nongovernmental solutions.
- 809 • Stakeholders at all levels should coordinate requirements and ensure resources are not
810 being over-tasked.
- 811 • Planners should identify resource shortfalls and solutions during steady-state
812 planning.
- 813 • Planners should be cognizant of resource depletion rates incurred in previous or
814 multiple events.

815 **HORIZONTAL INTEGRATION**

816 Protection activities integrate operations horizontally at the Federal, state, and local levels
817 and across private sector organizations in the following two ways:

- 818 • Activities are coordinated with nearby jurisdictions and regional partners that may
819 share authorities, resources, or information and support each other in delivering
820 Protection core capabilities. Protection activities also are coordinated across
821 functional areas within a jurisdiction, such as police, fire, public health, and public
822 works. Horizontal integration also occurs between and among government entities
823 and the private sector elements, community groups, and nongovernmental
824 organizations at all levels through partnerships and information sharing.
- 825 • At the Federal level, horizontal integration is achieved across the five mission areas
826 through the development of the frameworks, the Federal interagency operational
827 plans (IOPs), and the department-level operational plans. Specifically, all mission
828 areas coordinate their frameworks with each other, focusing on the three integrating
829 factors. These factors also are applied in the development and maintenance of IOPs
830 and the Federal department-level operational plans. Using these integrating factors
831 enables Protection partners to understand the relationships, such as interdependencies
832 and capabilities, among the five mission areas. For example, in the development of
833 IOPs, horizontal integration may reveal multiple mission areas designating the same
834 resources for their plans.

835 Horizontal integration also needs to occur within each mission area among the various
836 departments and agencies that comprise the respective mission area. For example, in the
837 Protection mission area, horizontal integration occurs between and among Federal Government
838 organizations and the private sector entities, nongovernmental organizations, and international
839 partners as appropriate at the mission-area level for the frameworks, IOPs, and department-level
840 operational plans.

841 **VERTICAL INTEGRATION**

842 Vertical integration is a function of coordinating protection activities, by mission area,
843 among Federal, state, and local governments. For example, States integrate their plans both with
844 their local jurisdictions and with the Federal departments that support them in protection
845 operations. Pertinent regional organizations also are included as essential elements of vertical

846 integration. In addition, all levels of government participate in joint protection exercises to
 847 ensure integration of these plans.

848 **6.0 PLANNING GUIDANCE**

849 This section presents guidance on the development of operational planning to execute
 850 effective Protection operations in support of the National Protection Framework.

851 **FEDERAL INTERAGENCY OPERATIONAL PLAN**

852 Presidential Policy Directive 8 requires a Federal interagency operational plan (IOP) to
 853 support the National Protection Framework. The IOP should leverage current and past planning
 854 efforts to cover the delivery of the protection capabilities.

855 The Protection IOP will accomplish the following:

- 856 • Describe the concept of operations for integrating and synchronizing existing
 857 national-level Federal capabilities to support Federal, state, and local Protection
 858 preparedness plans.
- 859 • Identify processes to resolve overlapping or conflicting authorities.
- 860 • Include a list of steady-state, enhanced steady-state, and pre-incident plans that
 861 require the authorities and resources of more than one Federal department or agency
 862 and other stakeholders.
- 863 • Describe how Protection capabilities will be managed and delivered to support the
 864 whole community, including those with access and functional needs. Identify the
 865 resources and partners required to deliver those capabilities and the means of
 866 delivering them.
- 867 • Specifically address the following:
 - 868 ○ Protection planning assumptions for steady-state and enhanced steady-state
 869 activities.
 - 870 ○ Each of the Protection mission activities.
 - 871 ○ Identification of Federal departments and agencies as primary and supporting
 872 organizations for each of the mission activities based on existing authorities.
 - 873 ○ Integration and synchronization of existing Federal interagency planning that
 874 facilitates the delivery of Protection-related core capabilities.
 - 875 ○ Processes for ongoing interagency coordination, planning, information
 876 sharing, and program implementation that require the simultaneous
 877 implementation of one or more of the existing plans.
 - 878 ○ Communications policies, procedures, and capabilities for intra-agency and
 879 interagency communications support across the different mission areas.
 - 880 ○ Actions to be taken by specific coordinating structures responsible for
 881 ensuring the delivery of Protection core capabilities.

- 882 ○ Protection integration with and support for established coordinating structures
883 that deliver Protection core capabilities and resources during response and
884 recovery.

885 ***IOP Structure/Contents***

886 The recommended structure, contents, and developmental guidance for interagency
887 operational plans are described in detail in the National Planning System document. The
888 Protection IOP will describe how the Protection mission activities will be accomplished. The
889 IOP will include, but is not limited to, the following:

- 890 • A detailed description of critical tasks and responsibilities of Federal departments
891 with a role in protection activities.
- 892 • A description of how the Protection mission area will synchronize with the
893 operational activities of the other mission areas.
- 894 • Resource, personnel, and sourcing requirements.
- 895 • Objectives based on the National Preparedness Goal.
- 896 • Specific annexes for each Protection activity, describing the concept of operations
897 and other operational details necessary to describe how the relevant coordinating
898 structure will deliver the resources and services associated with that core capability.

899 ***IOP Development***

900 In accordance with PPD-8, the Secretary of Homeland Security will coordinate the
901 development of the interagency operational plan in collaboration with all Federal departments
902 and agencies that play a role in the implementation of the Protection Framework. Exhibit 7
903 below identifies the primary coordinating agencies/departments for each of the identified mission
904 activities.

905 Primary coordinating agencies/departments are responsible for the following:

- 906 • Identifying cooperating agencies and departments that have statutory, regulatory, and
907 voluntary roles and responsibilities related to Protection activities.
- 908 • Identifying and addressing any potential gaps and overlaps in Protection activities.
- 909 • Synchronizing policies and procedures for the development and delivery of the
910 Protection core capabilities.
- 911 • Developing sections of the IOP related to their Protection activities.
- 912 • Providing guidance to agencies and department to assist in the development of
913 department-level operational plans.
- 914 • Establishing a basis for the measurement of the Protection core capabilities.

915

Exhibit 7: Primary Coordinating Agencies/Departments by Protection Mission Activity

Row	Protection Mission Activity	Primary Coordinating Agencies/Departments
1	Defense Against WMD Threats	Department of Defense Department of Energy Department of Health and Human Services Department of Homeland Security Department of Justice
2	Defense of Agriculture and Food	Department of Agriculture Department of Health and Human Services Department of Homeland Security
3	Critical Infrastructure Protection	Department of Homeland Security
4	Protection of Key Leadership and Events	Department of Homeland Security Department of Justice
5	Border Security	Department of Homeland Security Department of State
6	Maritime Security	Department of Homeland Security
7	Immigration Security	Department of Homeland Security
8	Transportation Security	Department of Homeland Security Department of Transportation
9	Cybersecurity	Department of Homeland Security Department of Justice
10	Health Security	Department of Health and Human Services

916 ***IOP Review Requirements***

917 All Federal departments and agencies with representation on the Transborder Security
918 Interagency Policy Committee will review the IOP addressing Protection, adjudicate policy-level
919 issues, and approve the IOP.

920 The Secretary of Homeland Security will review and update the IOP at least every three
921 years or following major exercises, real-world events, or major revisions to the pertinent
922 framework.

923 In accordance with the guidance from the PPD-8 Implementation Plan, the first edition of
924 each IOP must be submitted to the President of the United States not later than September 25,
925 2012.

926 **DEPARTMENT-LEVEL OPERATIONAL PLANS**

927 As described in the PPD-8 Implementation Plan, each executive department and agency
928 will develop and maintain deliberate department-level operational plans, as determined by the

929 respective department or agency, to deliver Protection core capabilities to fulfill the
 930 organization’s responsibilities described in the IOPs.

931 Departments and agencies may use existing plans, protocols, or standard operating
 932 procedures or guides for the development of such plans. Each department or agency determines
 933 its own planning requirements and decides whether its components and/or agencies need to
 934 develop subordinate operational plans.

935 Department-level operational plans identify specific critical tasks and responsibilities,
 936 including how to meet resource requirements and other specific provisions addressed in the
 937 IOPs. Department-level operational plans also utilize the integrating factors for Protection—
 938 addressing risk, planning and exercising coordination and communication procedures, and
 939 sharing resources—and Protection core capabilities.

940 ***Department-Level Operational Plan Structure/Contents***

941 Department-level operational plans will include, but are not limited to, the following:

- 942 • A detailed concept of operations supporting the IOP and delivering required
 943 Protection core capabilities through the appropriate coordinating structure.
- 944 • A description of specific tasks and responsibilities through which the
 945 department/agency will support the goals of the IOP and deliver the required
 946 Protection core capabilities through the designated coordinating structure.
- 947 • Detailed resource and sourcing requirements.
- 948 • Detailed communications procedures and requirements for execution of department
 949 missions.
- 950 • A specific schedule and asset/resource list for the application of department or agency
 951 resources and services.
- 952 • Objectives.
- 953 • Logistics for executing the required tasks and delivering the requisite resources and
 954 services.
- 955 • Annexes, as required, to address department or agency-unique issues in supporting
 956 the delivery of Protection core capabilities through the designated coordinating
 957 structure(s).

958 ***Department-Level Operational Plan Initial Development and Review Cycle***

959 The head of each department or agency will determine the number and scope of plans
 960 required to support the department’s/agency’s responsibilities under the pertinent IOP(s) and will
 961 establish a deadline of no more than 2 years following approval of the IOP(s). The head of each
 962 department or agency also will determine the schedule for review and revision of the
 963 department’s/agency’s department-level operational plans. The review cycle will define the
 964 approval process as well as the means and methods for assuring the participation of all relevant
 965 stakeholders in reviewing and adjudicating issues associated with the plans.

966 **7.0 FRAMEWORK MAINTENANCE AND REVIEW CYCLE**

967 The Protection Framework includes a process for review, periodic interim updates as
 968 required, and regularly scheduled partial reviews and reissuance as directed by the Secretary of
 969 Homeland Security. First-edition frameworks will be reviewed within 18 months of release, and
 970 then every four years thereafter. Reviews will engage the whole community to solicit feedback
 971 and recommendations.

972 DHS oversees the review and maintenance process for the Protection Framework. The
 973 revision process includes developing or updating any documents necessary to carry out
 974 capabilities. This Framework is reviewed to:

- 975 • Assess and update core capabilities in support of Protection goals and objectives.
- 976 • Ensure that it adequately reflects the organization of responsible entities.
- 977 • Ensure that it is consistent with the other four mission areas.
- 978 • Update processes based on changes in the national risk management environment.
- 979 • Incorporate lessons learned and effective practices from day-to-day operations,
 980 exercises, and actual incidents and alerts.
- 981 • Reflect progress in the Nation’s Protection mission activities, as well as changes to
 982 national priorities and guidance, critical tasks, sector organization, or national
 983 capabilities.

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

988 **MAINTENANCE AND UPDATES**

989 **Types of Changes.** Changes include the addition of new or supplementary material and
 990 deletions. No proposed change should contradict or override authorities or other plans contained
 991 in a statute, Executive order, or regulation.

992 **Coordination and Approval.** While DHS is the lead Federal department for the
 993 Protection Framework development and maintenance, any Federal department or agency with
 994 assigned responsibilities under this Framework may propose a change. DHS is responsible for
 995 capturing and coordinating the review and approval of all proposed modifications with
 996 Protection partners, as appropriate. Policy changes will be coordinated and approved through the
 997 Interagency Protection Coordination Group.

998 **Notice of Change.** DHS will issue an official Notice of Change for each interim revision
 999 to this Framework. After publication, the modifications will be considered part of the Protection
 1000 Framework for planning purposes pending a formal revision and reissuance of the entire
 1001 document. Interim changes can be further modified or updated using this process. (Periodic
 1002 updates resulting from the annual review process do not require the formal Notice of Change.)

1003 **Distribution.** DHS will distribute Notices of Change to Federal, state, and local
 1004 government entities as well as specific private sector partners. Notices of Change to other
 1005 organizations will be provided upon request.

1006 **Reissuance.** DHS will coordinate full reviews and updating of this Framework every four
1007 years or more frequently, if directed by the Secretary of Homeland Security. The review and
1008 updating process will consider lessons learned and best practices identified during
1009 implementation in each sector and will incorporate the periodic changes and any new
1010 information technologies. DHS will distribute revised documents for interagency review and
1011 concurrence.

1012 **8.0 CONCLUSION**

1013 The responsibility for Protection builds from the individual and the community to local
1014 jurisdictions, state governments, and the Federal Government. This Framework assists the whole
1015 community in protecting against the greatest risks to our Nation from all hazards in a manner that
1016 allows our interests, aspirations, and way of life to thrive.

1017 This Framework provides individual residents, communities, and governmental, private
1018 sector, and nongovernmental organization decision makers with an understanding of the full
1019 spectrum of Protection mission activities and what they can do to ensure our Nation is optimally
1020 protected from man-made and natural disasters. Initiatives based on Protection mission activities
1021 and core capabilities help guide a community to create conditions for a safer, more secure, and
1022 more resilient Nation by enhancing Protection through cooperation and collaboration.