

PRESIDENTIAL POLICY DIRECTIVE/PPD-8 REFRESH

WORKING DRAFT—PROTECTION FEDERAL INTERAGENCY OPERATIONAL PLAN

NATIONAL ENGAGEMENT

August 3, 2015

Attached for your review is the working annotated outline of the Protection Federal Interagency Operational Plan (FIOP), first edition. The Protection FIOP describes the concept of operations for integrating and synchronizing existing national-level Federal capabilities to support local, state, tribal, territorial, insular area, and Federal plans. The Federal protection processes and guiding principles contained in this FIOP provide a structured and unifying approach that is flexible and adaptable to specific Protection mission requirements.

As part of the FIOPs National Engagement Period, this annotated outline of the Protection FIOP is being widely distributed for review and feedback. The draft Protection FIOP proposes a new concept of operations for the Protection mission. We are particularly interested in your assessment of how this can strengthen the Protection mission, and improve the way that protection capabilities support other mission areas.

To ensure all feedback is properly handled, reviewers are asked to use the provided feedback submission form located at <https://www.fema.gov/learn-about-presidential-policy-directive-8> to submit feedback and recommendations. Please provide any comments and recommendations, using the submission form, to PPD8-Engagement@fema.dhs.gov by **Wednesday, September 2 2015 at 5:00 PM EDT**.

The feedback received supports the development of the first edition of the Protection FIOP. Please distribute the draft to any applicable partners, stakeholder, or individuals.

We look forward to receiving your feedback and thank you for your continued contributions on this important endeavor.

V/R,

National Integration Center

Table of Contents

2	TABLE OF CONTENTS	I
3	INTRODUCTION	1
4	Purpose	2
5	Scope	3
6	Mission	4
7	Organization.....	4
8	Planning Assumptions	4
9	CONCEPT OF OPERATIONS	5
10	Steady State Protection.....	5
11	Protection Escalation.....	6
12	Coordination Mechanisms	8
13	Core Capabilities	11
14	Coordinating Activities.....	12
15	ANNEX A: ALIGNMENT	16
16	Integration with Existing Plans, Strategies, & Doctrine.....	16
17	Relationship with Other Mission Area National Frameworks & IOPs.....	16
18	Appendix 1 to Annex A: Protection Federal Leadership Group Charter	19
19	Appendix 2 to Annex A: Networked Coordination.....	20
20	ANNEX B: PROTECTION PLANNING	21
21	Planning	21
22	Public Information & Warning.....	21
23	Operational Coordination.....	22
24	Appendix 1 to Annex B: Access Control and Identity Verification.....	23
25	Appendix 2 to Annex B: Intelligence and Information Sharing.....	24
26	Appendix 3 to Annex B: Interdiction and Disruption	26
27	Appendix 4 to Annex B: Screening, Search, and Detection	27
28	Appendix 5 to Annex B: Physical Protective Measures	28
29	Appendix 6 to Annex B: Risk Management for Protection Programs and Activities	29
30	Appendix 7 to Annex B: Cybersecurity	30
31	Appendix 8 to Annex B: Supply Chain Integrity and Security	31
32	ANNEX C: COORDINATING ACTIVITIES	32
33	Appendix 1 to Annex C: Border Security	34
34	Appendix 2 to Annex C: Critical Infrastructure Protection.....	35
35	Appendix 3 to Annex C: Cybersecurity	47
36	Appendix 4 to Annex C: Defense Against Weapons of Mass Destruction (WMD) Threats	48
37	Appendix 5 to Annex C: Defense of Agriculture and Food	50
38	Appendix 6 to Annex C: Health Security.....	55
39	Appendix 7 to Annex C: Immigration Security	56
40	Appendix 8 to Annex C: Maritime Security	57
41	Appendix 9 to Annex C: Protection of Key Leadership and Events.....	59
42	Appendix 10 to Annex C: Transportation Security.....	60
43	ANNEX D: SELECTED GLOSSARY/LEXICON	63

44 **Introduction**

45 The National Preparedness System outlines an organized process for the whole community to
 46 achieve the National Preparedness Goal. The National Preparedness System integrates efforts across
 47 the five preparedness mission areas—Prevention, Protection, Mitigation, Response, and Recovery –
 48 in order to achieve the goal of a secure and resilient Nation. The National Preparedness System
 49 includes a set of Federal Interagency Operational Plans (FIOPs)—one for each mission area—that
 50 provide further detail regarding roles and responsibilities, specifies the critical tasks and identifies
 51 resourcing requirements for delivering core capabilities.

52 This FIOP builds upon the National Protection Framework that sets the strategy and doctrine for how
 53 the whole community builds, sustains, and delivers the Protection core capabilities identified in the
 54 National Preparedness Goal. This FIOP describes the concept of operations for integrating and
 55 synchronizing existing national-level Federal capabilities to support local, state, tribal, territorial,
 56 insular area, and Federal plans, and is supported by Federal department-level operational plans,
 57 where appropriate. The concept of operations and supporting tasks contained in the Protection FIOP
 58 are scalable, flexible, and adaptable, allowing the FIOP to be used across the range of protection
 59 mission activity. Concepts of operations and/or tasks may be modified, added, or deleted depending
 60 upon the risk, mission activity, or threat.

61 The FIOP-Protection summary is provided below.

62 **Table 1**

The FIOP-Protection:	The FIOP-Protection <i>is not/does not</i> :
Is a document that provides guidance and a concept of operations to facilitate the development of plans.	A contingency or implementation plan based on threat(s) or scenario(s).
Describes a Federal approach that Departments and Agencies can apply to align protection mission activity.	Establish requirements on how Federal Department/Agencies will execute their Protection requirements.
Addresses protection for Federal Department/Agency requirements, and informs State, local, tribal, territorial, and private sector partners of how the capabilities will be delivered.	Address State, local, tribal, territorial, private sector, and individual roles and responsibilities.
Includes security measures taken in response to emergent threats or elevated risks	Include discussion of protection coordination and operations following an incident [or disaster?], which is covered in the National Response Framework and FIOP – Response.
Recognizes that protection of key leaders is limited to current and former Presidents, Vice Presidents, their families, and others granted such protection under Title 18 U.S.C. Sections 3056 and 3056A.	Address protection of other Federal, State, local, territorial, and/or tribal key leaders.

63 Additional Presidential Policy Directive (PPD)-8 requirements:

64 Where needed, each executive department and agency will develop and maintain deliberate
 65 department-level operational plans to deliver capabilities to fulfill responsibilities under the
 66 frameworks and FIOPs.

67 Departments and agencies may use existing plans, protocols, standard operating procedures (SOPs),
68 or standard operating guides (SOGs) for the development of such plans; these should be updated as
69 needed.

70 *Purpose*

71 This document guides the way that the United States Government delivers core capabilities to protect
72 people, critical assets, systems, and networks against the greatest risks to the Nation.¹ The protection
73 mission comprises a broad range of homeland security activity, and the Protection FIOP serves as a
74 reference point that connects plans to plans and mission activities to mission activities. When Federal
75 departments and agencies must conduct protection activities jointly, or act independently based on
76 shared information, this FIOP provides a Federal standard for how such actions are organized and
77 executed.

78 As an operational plan, the Protection FIOP describes how federal departments and agencies acting
79 under distinct authorities conduct protection operations in coordinated manner. The content of the
80 protection concept of operations derives from the principles and concepts in the National Protection
81 Framework and serves as a common reference for the development of contingency or mission
82 activity specific protection plans.

83 The inherent decentralization of activities in the protection missions amplifies the importance of
84 information sharing and shared situational awareness for Federal partners. For example, critical
85 infrastructure protection activities coordinated through sector specific plans are conducted under
86 discrete authorities and independently from activities focused on defense against weapons of mass
87 destruction (WMD) threats. However, in order to effectively manage the protection risks, each of
88 these mission activities relies on a structure of information sharing and coordination. The same is
89 true for heightened awareness, and escalated coordination of protection activities that may follow
90 from elevated threats or terrorist attacks. The concept of operations described in this FIOP provides
91 the necessary Federal structure for managing these protection concerns.

92 Protection activities are conducted predominantly as “steady-state” operations, meaning they are
93 ordered by the normal, day to day conduct of protection mission activities and the delivery of the
94 protection core capabilities. But protective actions are also delivered during times of elevated threat,
95 requiring departments and agencies to align activity. This FIOP provides operational guidance for
96 both steady state alignment of protection activity and the operational arrangements that characterize
97 enhanced or escalated decision-making and protective posture.

¹ Core capabilities are defined as “distinct critical elements necessary to achieve the National Preparedness Goal.”

98 Protection capabilities are often called upon to support response and recovery activities. During these
 99 situations, protection integrates within the mission and operational structures of response and
 100 recovery. This FIOP provides an overview of the way that protection connects to other mission areas,
 101 with special attention to the Prevention Mission, which shares some core capabilities and mission
 102 activities with Protection.

103 The Prevention and Protection mission areas are closely linked in that Protection activities may
 104 uncover an imminent terrorist threat during the conduct of their steady state Protection missions, such
 105 as screening, search, and detection operations at borders and ports of entry, at special events, etc.
 106 Such threats when detected may require urgent action to resolve the immediate situation, such as
 107 reporting, detention, or arrest. In such cases, upon resolution of the immediate situation, the
 108 information and investigation must be seamlessly transition to the Prevention mission so the threat
 109 can be fully investigated in order to identify additional plots, accomplices, or other attacks.

110 *Scope*

111 This document is written for and is applicable across all Federal Departments/Agencies involved in
 112 protecting people, critical assets, systems, and networks against the greatest risks to the Nation.²
 113 Additionally, it serves as a guide to the Federal Government delivery of protection core capabilities
 114 for State, local, tribal and territorial governments; the private sector' non-governmental organizations
 115 (NGOs); and American citizens.

116 The scope of the FIOP-Protection is summarized in Table 2.

117

Table 2

Scope Element	Description
Purpose	Describe how the Federal government will deliver core capabilities.
Audience	Federal Departments/Agencies involved in protecting people, critical assets, systems, and networks against the greatest risks to the Nation. Additionally, it informs the U.S. "Whole of Community" ^{4F} involved in Protection and Protection-related activities.
Concept of Operations	Lorem Ipsum
Core Capabilities	Lorem Ipsum
Coordination	Lorem Ipsum

² The Nation includes the 56 U.S. States, territories and possessions as defined in the Homeland Security Act of 2002 (HSA 2002), as amended.

Scope Element	Description
Activities	
Alignment	Lorem Ipsum

118 *Mission*

119 The Federal Government leads, coordinates, and delivers Protection core capabilities in order to
120 secure the homeland against acts of terrorism and manmade or natural disasters.

121 *Organization*

122 Lorem Ipsum [This section will summarize the overall organization of the FIOP, and include a
123 description of how this FIOP is tied to the National Planning system, and the architecture of Federal
124 Protection plans.]

125 *Planning Assumptions*

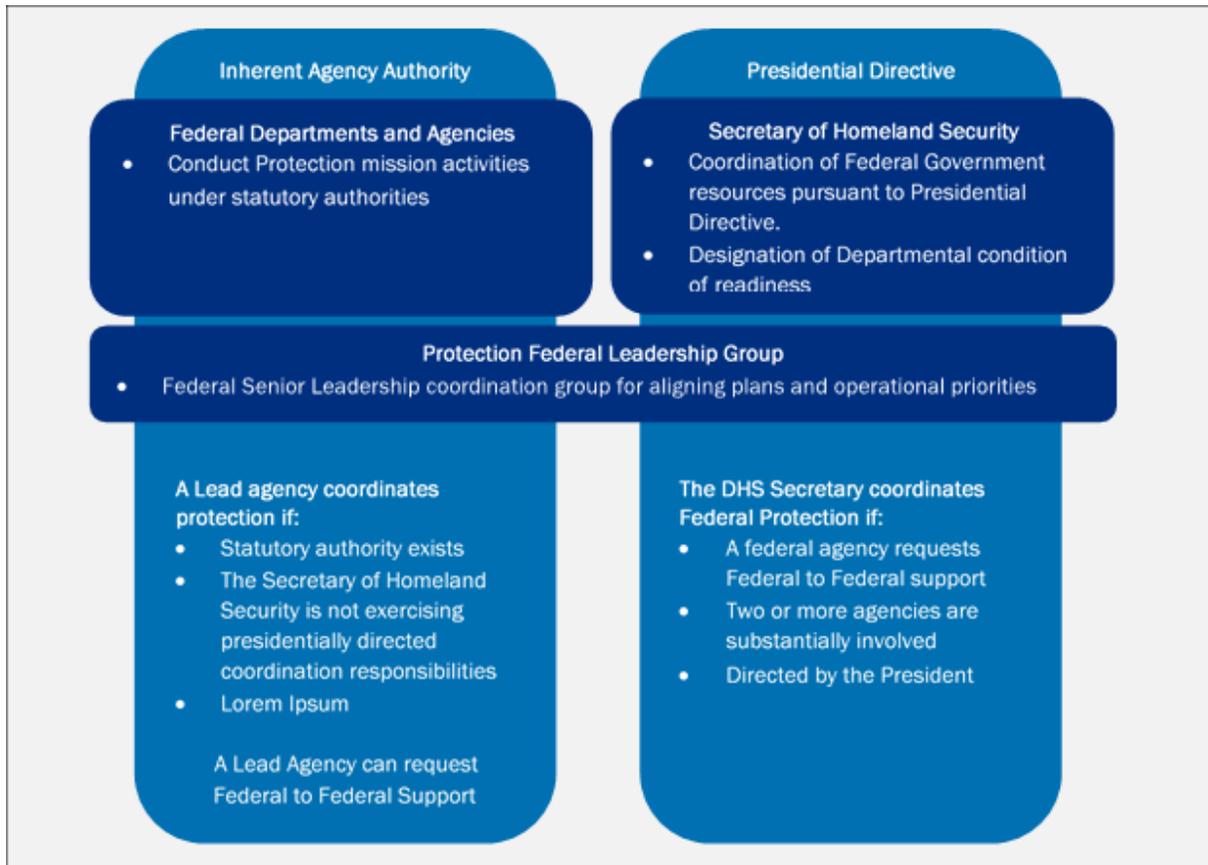
126 Assumptions consist of information accepted by planners as true in the absence of facts. Assumptions
127 are not predictions. Assumptions are only used when facts are unavailable. Using assumptions allows
128 planners to further define the scenario, identify potential response requirements, and move forward
129 with the planning process. Assumptions are a baseline set for planning purposes, and they do not take
130 the place of specific activities or decision points related to specific risks or mission activities. The
131 following planning assumptions assist in the development of an operational environment for this
132 FIOP. During protection operations, assumptions are validated as facts, as necessary.

133 Nothing in this document is intended to alter or impede the ability to carry out the authorities of
134 executive departments and agencies to perform their responsibilities under law and consistent with
135 applicable legal authorities and other Presidential guidance. Nothing in this FIOP is intended to
136 interfere with the execution of the roles and responsibilities and the authorities of individual
137 departments and agencies concerning counterterrorism, counterintelligence, law enforcement, or
138 other related missions.

- 139 ▪ Protection mission activities are conducted independently under existing authorities
- 140 ▪ Protection activities take place continuously and may be implemented concurrently with
141 Prevention, Mitigation, Response, and Recovery capabilities.
- 142 ▪ Protection resources are acquired, allocated, and assigned through the normal Federal budget and
143 program processes.
- 144 ▪ Protection responsibilities are decentralized and capabilities are distributed among Federal
145 departments and agencies, depending on the mission activity.
- 146 ▪ Priorities to employ Federal Protection capabilities will change based on the situation during
147 escalated decision-making conditions.
- 148 ▪ The Protection Federal Leadership Group will serve as the coordinating body for addressing
149 emergent or persistent Protection issues across Federal departments and agencies.
- 150 ▪ While conducting responding to a suspected or actual terrorist incident, protection, prevention
151 and response mission operations will be ongoing concurrently. Unity of effort will be required
152 with Prevention and Response mission areas to resolve threats, save lives, and protect property.
- 153 ▪ All possible terrorist incidents will be treated as an act of terrorism until determined otherwise.

154 **Concept of Operations**

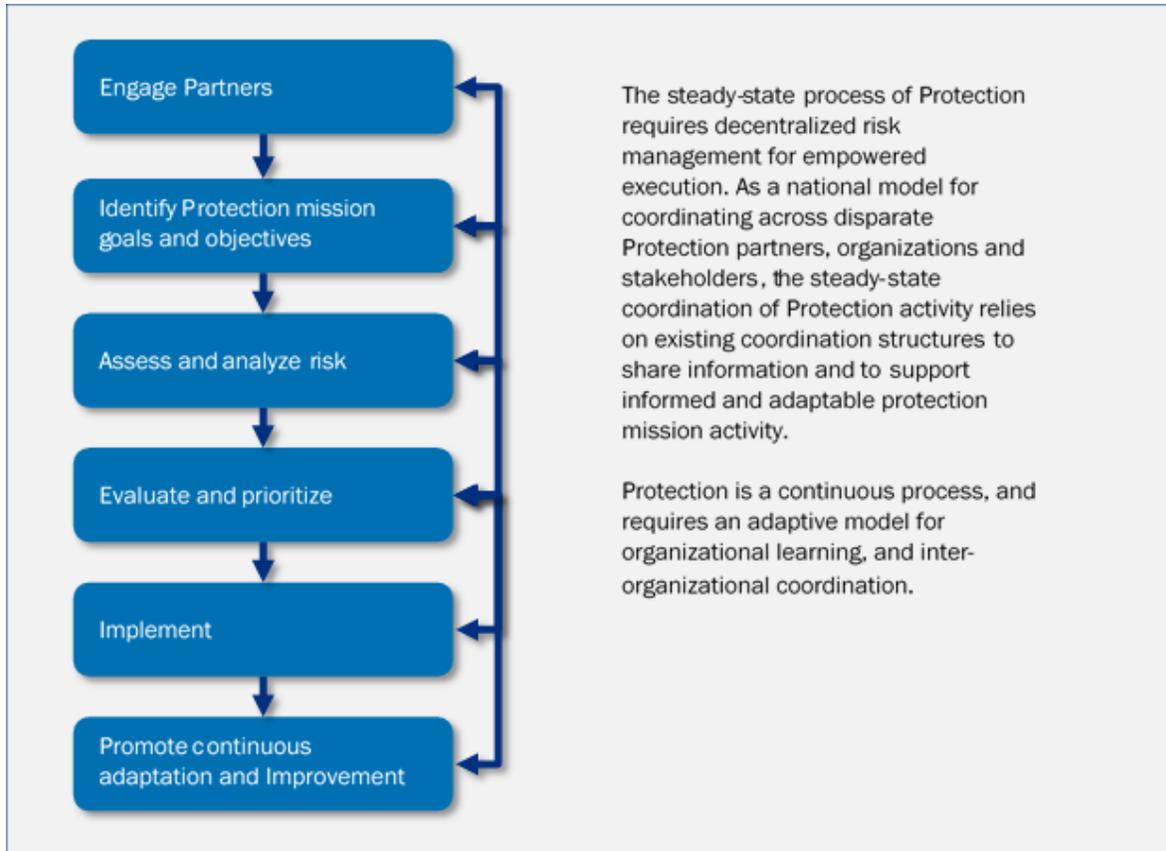
155 The Protection FIOP is an all-hazards plan that describes how the Federal Government will align
 156 Protection Mission Activity. This document describes how the Federal departments and agencies
 157 work together to deliver the Protection core capabilities during steady-state and escalated decision
 158 making operations that flow from emergent threats and elevated risks. Government and private sector
 159 partners may use the FIOP-Protection to inform and enable ongoing Protection planning, training,
 160 and exercising within their jurisdictions or organizations.



161
 162 **Figure 1**

163 **Steady State Protection**

164 Lorem ipsum [This section will describe the way that protection occurs and is coordinated during
 165 steady state operations]



166

167

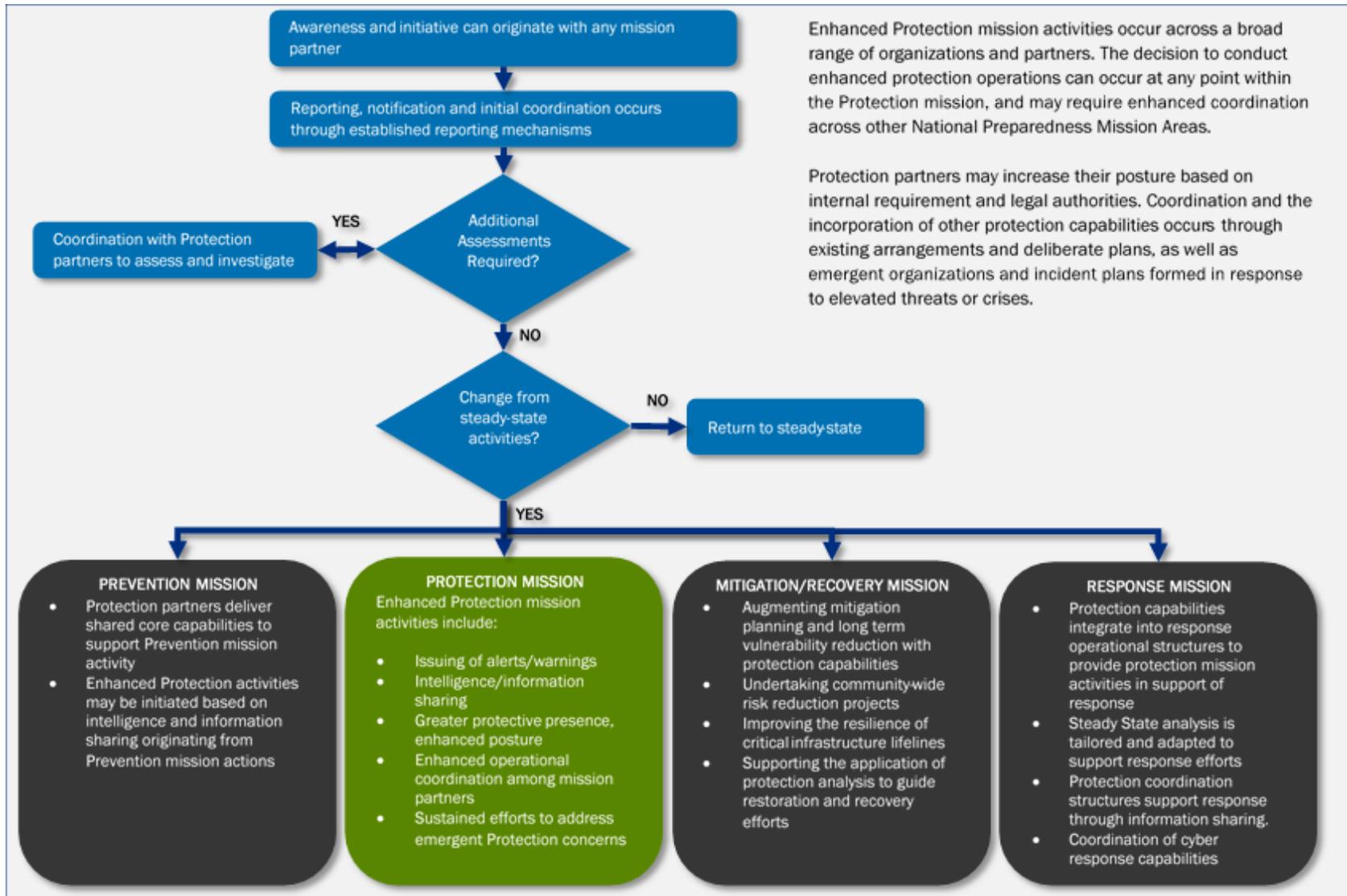
Figure 2

168 *Protection Escalation*

169 Lorem Ipsum [focus here on taking the generalized process and concept in the National Protection
170 Framework, and identifying the Federal process and approach to escalation and decision making]

171

172



173

174

Figure 3

175 **Coordination Mechanisms**

176 As described in the National Protection Framework, adaptable coordinating structures are essential to
177 align the key roles and responsibilities to deliver the core capabilities for the Protection mission area.
178 Coordinating structures also provide the mechanisms to develop and deliver core capabilities.
179 National Protection relies on a robust array of existing coordinating structures.

180 **Aligning Coordination Mechanisms**

181 Lorem Ipsum

182 At the Federal level, an array of coordinating structures exists to facilitate partnerships, planning,
183 information sharing, and resource and operational synchronization across all aspects of the Protection
184 mission area. This section focuses on the policy-level coordination conducted through White House
185 leadership, public-private partnerships, and those structures that are in place or need to be established
186 to ensure a coordinated approach to Protection across the whole community.

187 The Federal Government promotes coordination within and across the Protection mission area
188 through a wide range of coordinating structures. Under the Protection Framework, various Federal
189 departments or agencies assume primary coordinating roles based on their authorities, the specific
190 mission activities, and the nature of the threat or hazard. These Federal departments and agencies
191 provide the basis for the ongoing coordination and collaboration that will be required to promote
192 implementation and ensure the ongoing management and maintenance of the Protection Framework
193 and other Protection preparedness requirements established through PPD-8. As needed, the Secretary
194 of Homeland Security will convene, as appropriate, a meeting or meetings among Federal department
195 and agency representatives to discuss and consider the coordination of Protection mission activities,
196 focusing on the following:

- 197 ■ Preparedness planning and coordination in accordance with the National Protection Framework
198 and other PPD-8 implementation efforts
- 199 ■ Information sharing pertinent to the Protection mission activities
- 200 ■ Collaboration across the whole community
- 201 ■ Addressing common concerns and recommending courses of action
- 202 ■ Integration with Prevention, Mitigation, Response, and Recovery by coordinating with similar
203 groups within those mission areas.

204 **Protection Federal Leadership**

205 The Federal Government will establish a Protection Framework Leadership Group (ProFLG) to
206 provide a national coordinating structure focused on integrating Federal efforts to deliver Protection
207 core capabilities (See ProFLG Charter in Annex A, Appendix 1). The ProFLG will consist of senior
208 leaders designated by Federal departments and agencies to coordinate collectively the diverse
209 protection efforts implemented across the Nation. The ProFLG will be responsible for monitoring
210 and assessing the effectiveness of Protection core capabilities and work to improve the efficiency and
211 effectiveness of Federal interagency coordination practices and operations regarding how the Nation
212 manages risk through Protection core capabilities.

213 The ProFLG will work to advance the principles and objectives of the National Protection
214 Framework (NPF) and this Protection FIOP. It will provide a forum for information exchange, share
215 best practices and updates on programs and policies that directly affect the NPF, and set the strategic
216 national direction and integrated priorities relative to implementation of the NPF.

217 ***Activation for Protection Escalation***

218 When needed and appropriate, the ProFLG, in consultation with the National Security
219 Council/Domestic Resilience Group, will coordinate interagency decision-making during periods of
220 escalated deployment of protection capabilities. It will elevate unresolved policy, program, and
221 operational issues to the Disaster Resilience Group (DRG), make recommendations on interagency
222 protection policies and practices during routine and escalated periods, and provide guidance on
223 resolving disagreements among ProFLG members.

224 In support of PPD-8 requirements and consistent with the National Infrastructure Protection Plan
225 (NIPP), the ProFLG will be chaired by the Undersecretary of the National Protection and Programs
226 Directorate (NPPD) or designee. The Group will be managed through a Secretariat that rotates
227 annually among member departments or agencies.

228 **National Security Council**

229 The National Security Council (NSC) is the principal forum for consideration of national and
230 homeland security policy issues requiring Presidential determination. The NSC, which brings
231 together Cabinet officers and other department or agency heads as necessary, provides national
232 strategic and policy advice to the President on a range of Protection issues.

233 **Trans-border Security Interagency Policy Committee**

234 The Trans-Border Security Interagency Policy Committee (IPC) provides policy coordination,
235 dispute resolution, and periodic in-progress reviews for the development of national-level
236 performance objectives to achieve the National Preparedness Goal's core capabilities for Protection,
237 as well as for the development of the National Protection Framework.

238 **Federal Departments and Agencies**

239 The Federal Government promotes coordination within and across the Protection mission area
240 through a wide range of coordinating structures. Under the Protection Framework, various Federal
241 departments or agencies assume primary coordinating roles based on their authorities, the specific
242 mission activities, and the nature of the threat or hazard. These Federal departments and agencies
243 provide the basis for the ongoing coordination and collaboration that will be required to promote
244 implementation and ensure the ongoing management and maintenance of the Protection Framework
245 and other Protection preparedness requirements.

246 In addition to the Secretary of Homeland Security's responsibilities as described in Homeland
247 Security Presidential Directive (HSPD)-5, PPD-8 states, "The Secretary of Homeland Security is
248 responsible for coordinating the domestic all-hazards preparedness efforts of all executive

249 departments and agencies, in consultation with state, local, tribal, and territorial governments, NGOs,
250 private-sector partners, and the general public.”³ PPD-8 further states that the heads of all executive
251 departments and agencies with a role in Protection are responsible for national preparedness efforts
252 consistent with their statutory roles and responsibilities⁴

253 The Secretary of Homeland Security is the principal Federal official for domestic incident
254 management per HSPD-5.⁵ In executing this responsibility, the Secretary must remain aware of
255 incidents as they emerge and the actions taken by the Nation related to those incidents. The National
256 Operations Center (NOC) provides this service to the Secretary. The below graphic depicts how
257 information is coordinated from the local level to build a national common operating picture (COP).

258 **National-Level Partnership Councils**

259 The National Infrastructure Protection Plan (NIPP) promotes the use of a sector partnership model as
260 the primary organizational structure for coordinating infrastructure protection efforts and activities.
261 Federal Sector-Specific Agencies (SSAs) are responsible for critical infrastructure protection
262 activities in specified sectors. Each sector has built partnerships with sector stakeholders, including
263 facility owners and operators; Federal, state, and local government agencies; the law enforcement
264 community; trade associations; and state homeland security advisors.⁶ SSAs are responsible for
265 working with both public and private partners to develop protective programs and resilience
266 strategies.

267 The NIPP sector partnership model encourages formation of Sector Coordinating Councils (SCCs)
268 and Government Coordinating Councils (GCCs). Together, SCCs and corresponding GCCs create a
269 coordinated national structure for infrastructure protection within and across sectors. Additional
270 information on the coordinating councils can be found in the NIPP.⁷

³ White House, Presidential Policy Directive 8: National Preparedness, Washington, DC, March 30, 2011.

⁴ Specific statutory and other responsibilities for DHS and other Federal departments and agencies are identified in [MISSING WORDS] and its footnotes.

⁵ Except for those activities that may interfere with the authority of the Attorney General or the FBI Director, as described in PPD-8.

⁶ The Sector-Specific Agencies responsible for critical infrastructure protection for specified sectors were established under the authority of Homeland Security Presidential Directive 7 (HSPD-7), Critical Infrastructure Identification, Prioritization, and Protection and are identified in the National Infrastructure Protection Plan.

⁷ The National Infrastructure Protection Plan (NIPP).

271 For many of the Protection mission activities—defense of agriculture and food, critical infrastructure
272 protection, maritime security, transportation security, cybersecurity⁸, and health security—the
273 established sector, government, and coordinating councils and information-sharing mechanisms
274 provide the foundation for Protection planning, risk management, and the implementation of
275 protective programs for critical infrastructure.

276 **Integration of Federal Capabilities with Other Partners**

277 The US Government uses a variety of coordination mechanisms to ensure the Nation is protected
278 from all threats and all hazards. Because the Protection mission area is ongoing and does not stop,
279 coordination mechanisms must exist in a constant and flexible posture.

280 To this end, the Federal Government hosts a variety of regionally-focused, cross-capability forums to
281 combine and coordinate resources, authorities and mission to achieve the Protection mission.
282 Examples of these forums include the US Secret Service Electronic Crimes Task Forces and the
283 Federal Bureau of Investigation's (FBI) InfraGard.⁹ Department of Homeland Security (DHS) also
284 staffs Protective Service Advisers in the field that assists in information sharing and preparedness
285 activities across a variety of partners. These regional forums and imbedded personnel share
286 appropriate information with state and national bodies to ensure protection capabilities at all levels of
287 government are operating to achieve common goals and objectives.

288 **Core Capabilities**

289 Lorem Ipsum [This section will provide an overview of the Protection core capabilities within the
290 Federal sphere, and will point to the discrete core capability appendices to annex B as constructs for
291 Federal planning to develop and test federal capability based plans.]

⁸ The Cyber UCG [Unified Coordination Group] is an interagency and inter-organizational coordination body that incorporates public and private sector officials. It works during steady-state to ensure unity of NCCIC coordination and preparedness efforts and to facilitate the rapid response in case of a Significant Cyber Incident. The Cyber UCG is a pool of individuals that works to ensure centralized coordination and execution can take place effectively. It is composed of senior officials and staff that have been pre-selected by the leadership of their department, agency, or organization. Per DHS CS&C, NCIRP, p.16

⁹ FBI InfraGard is a partnership between the FBI and the private sector. InfraGard is an association of businesses, academic institutions, State and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States.

292

Table 3

Protection Core Capabilities	Description
Planning	
Public Information and Warning	
Operational Coordination	
Access Control and Identity Verification	
Intelligence and Information Sharing	
Interdiction and Disruption	
Screening, Search, and Detection	
Physical Protective Measures	
Risk Management for Protection Programs and Activities	
Cybersecurity	
Supply Chain Integrity and Security	

293 *Coordinating Activities*

294 Protection covers multiple spheres of operation. These stem from statutory authorities and existing
 295 federal coordination structures that are led, coordinated, and integrated by the Federal Government to
 296 secure the homeland against acts of terrorism and manmade or natural disasters. Protection mission
 297 activities are existing means of ordering and coordinating the Protection mission, and maintain plans,
 298 coordination structures and resource arrangements. The Protection FIOP describes the way that
 299 Departments and Agencies align separate Protection mission activities.

300 This FIOP contains separate Protection Activity Annexes that provide a description of Federal
 301 department and agencies responsibilities and coordinating structures for existing Protection mission
 302 activities as well as how they engage and contribute to the delivery of core capabilities discussed in
 303 the National Protection Framework. The Protection mission activities addressed in this FIOP are not
 304 an exhaustive or exclusive list. As Protection concerns emerge, the mission adapts and evolves to
 305 address them. The ten coordinating activities described in this FIOP are existing means of conducting
 306 Protection activity within distinct and established domains of operation.

307 The Protection mission activities and associated Annexes addressed in this FIOP are:

- 308 ▪ **Border Security.** Securing U.S. air, land, and sea ports and borders against the illegal flow of
309 people and goods, while facilitating the flow of lawful travel and commerce.
- 310 ▪ **Critical Infrastructure Protection.** Protecting the physical and cyber elements of critical
311 infrastructure. This includes actions to deter the threat, reduce vulnerabilities, or minimize the
312 consequences associated with a terrorist attack, natural disaster, or manmade disaster. Critical
313 Infrastructure Protection is an element of critical infrastructure security and resilience as detailed
314 in Presidential Policy Directive 21: Critical Infrastructure Security and Resilience.¹⁰
- 315 ▪ **Cybersecurity.** Securing the cyber environment and infrastructure from unauthorized or
316 malicious access, use, or exploitation while protecting privacy, civil rights, and other civil
317 liberties.
- 318 ▪ **Defense Against Weapons of Mass Destruction (WMD) Threats.** Protecting the Nation from
319 threats associated with WMD and related materials and technologies including their malicious
320 acquisition, movement, and use within the United States.
- 321 ▪ **Defense of Agriculture and Food.** Defending agriculture and food networks and systems from
322 all-hazards threats and incidents.¹¹
- 323 ▪ **Health Security.** Securing the Nation and its people to be prepared for, protected from, and
324 resilient in the face of health threats or incidents with potentially negative health consequences.
- 325 ▪ **Immigration Security.** Securing the Nation from illegal immigration through effective and
326 efficient immigration systems and processes that respect human and civil rights.
- 327 ▪ **Maritime Security.** Securing U.S. maritime infrastructure, resources, and the Marine
328 Transportation System from terrorism and other threats and hazards and securing the homeland

¹⁰ Critical infrastructure, as defined in PPD-21, includes those systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security; economy; public safety or health; environment; or any combination of these matters, across any jurisdiction. Critical infrastructure security and resilience addresses sectors along common functions that include chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

¹¹ Core capabilities for Protection align with policy established in HSPD 9: Defense of United States Agriculture and Food to include identifying and prioritizing sector critical infrastructure; developing awareness and early warning capabilities; mitigating vulnerabilities; and enhancing screening procedures.

329 from an attack from the sea, while preserving civil rights, respecting privacy and protected civil
330 liberties, and enabling legitimate travelers and goods to move efficiently without fear of harm or
331 significant disruption.

332 ■ **Protection of Key Leadership and Events.** Safeguarding government executive leadership from
333 hostile acts by terrorists and other malicious actors and to ensure security at events of national
334 significance.¹²

335 ■ **Transportation Security.** Securing U.S. transportation systems and the air domain against
336 terrorism and other threats and hazards, while preserving civil rights, respecting privacy and
337 protected civil liberties, and enabling legitimate travelers and goods to move without fear of harm
338 or significant disruption.

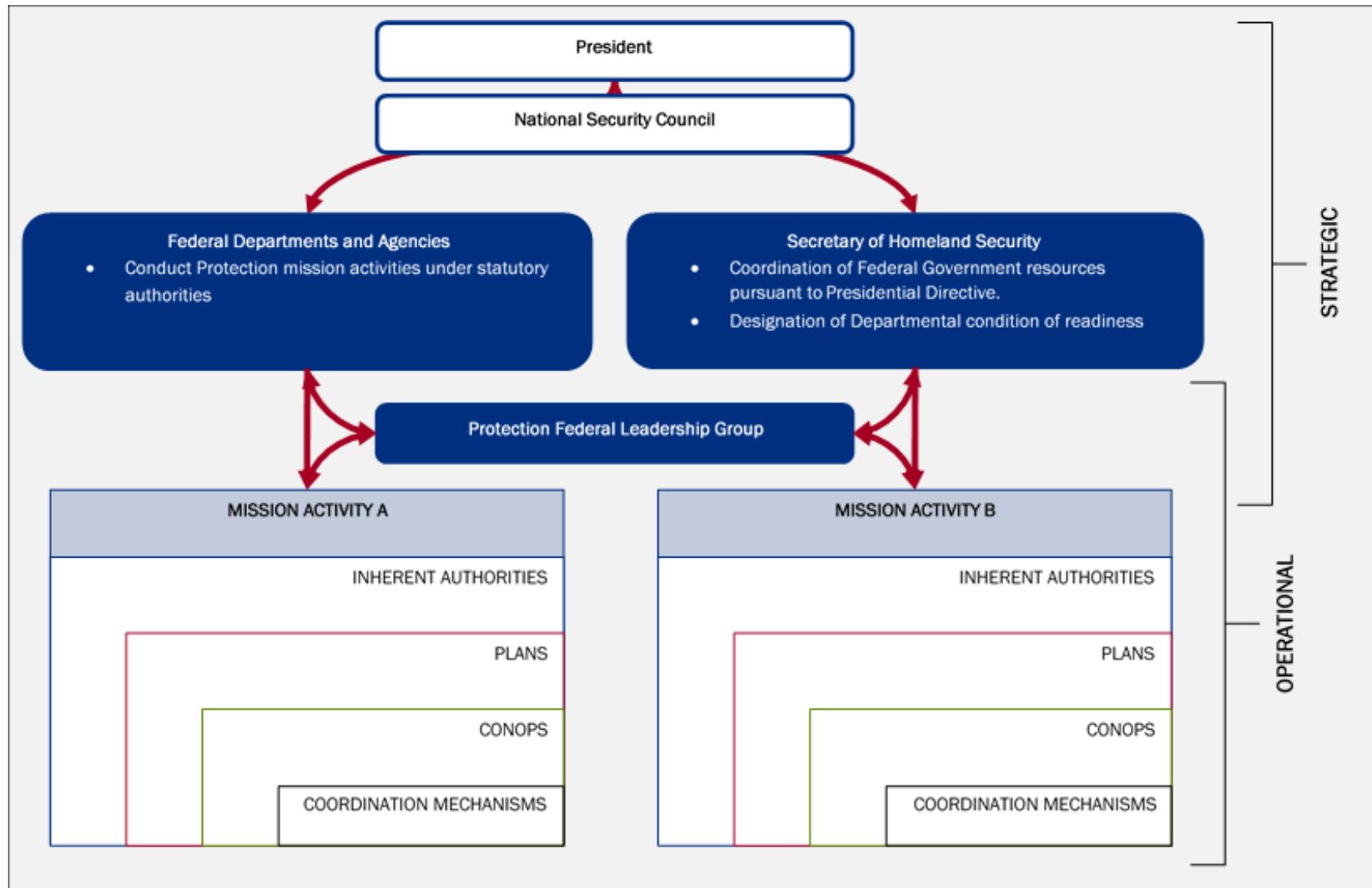
339 **Aligning Protection Mission Activity**

340 Lorem ipsum [This section provides an operational construct for how mission activities and
341 coordination structures are mutually aligned, and relate to the Protection Federal Leadership group as
342 the executive coordination structure for Protection operations.]

343

344

¹² 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 (NSSE) as defined in Title 18, U.S.C. Section 3056 and further clarified in PPD-22, and events assessed under the Special Event Assessment Rating (SEAR) process by the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) based on input from Federal, state, and local law enforcement entities.



345

346

Figure 4

347 **Annex A: Alignment**

348 *Integration with Existing Plans, Strategies, & Doctrine*

349 There are a number of existing plans, strategies, and doctrinal publications which provide the
350 foundation for the FIOP-Protection. These documents set the conditions to enable the Federal
351 government to deliver Protection core capabilities for each of the ten mission activities. Key
352 Protection related Federal plans, strategies, and doctrine are provided below (this list is not intended
353 to be all inclusive, and additional publications are provided for each of the ten mission activities in
354 Annex F):

355 *Relationship with Other Mission Area National Frameworks & IOPs*

356 The *National Preparedness Goal* is designed to prepare our Nation for the risks that will severely tax
357 our collective capabilities and resources. Each of the five mission areas serve as an aid in organizing
358 national preparedness activities, and do not constrain or limit integration across mission areas and
359 core capabilities. Mission area coordination (command, control, and communication) is conducted
360 through established organizational protocols with other mission areas. These mission areas exist
361 along a continuum, and there is a dynamic interplay between and among them and even some
362 commonality in the core capabilities essential to each (A summary of the mission area alignments is
363 provided in Table 4)

364

365

Table 4

Relationship of the Protection Mission Area with the Other Mission Areas				
	Prevention	Mitigation	Response	Recovery
Definition	The capabilities necessary to avoid, prevent, or stop a threatened or actual act of terrorism. For the purposes of the prevention framework called for in PPD-8, the term “prevention” refers to preventing imminent threats.	The capabilities necessary to reduce loss of life and property by lessening the impact of disasters.	The capabilities necessary to save lives, protect property and the environment, and meet basic human needs after an incident has occurred.	The capabilities necessary to assist communities affected by an incident to recover effectively.
Alignment	The Prevention mission area focuses on those intelligence, technical, and law enforcement actions which prevent an adversary from carrying out an attack within the United States when the threat is imminent in order to thwart an initial or follow-on terrorist attack. Protection activities, on the other hand, focus on measures that detect, deter, and/or disrupt terrorist surveillance, planning, and/or execution activities or deter and disrupt other threats and hazards and, like mitigation, focus on minimizing the consequences of significant events. In some cases, the same capabilities that are used for protection functions are also used in prevention operations. Other activities considered preventative, such as disease prevention and cybersecurity, fall under the Protection	The Mitigation and Protection Mission Areas work together to ensure the nation is resilient. Activities in the Mitigation and Protection missions typically are performed in a steady-state or well before an event. Protection places particular emphasis on security and deterring threats, while mitigation emphasizes achieving resilience by reducing vulnerabilities. Both seek to minimize consequences and include critical infrastructure security and resilience. Risk analysis is necessary to effectively design successful strategies for mitigation and protection. Integration of risk information, planning activities, and coordinating structures reduces duplication of effort and streamlines risk management actions in both mission areas	The Response and Protection Mission Areas will occur concurrently. Protection does not cease during Response. Protection capabilities deployed to support response efforts conform to and integrate into response organizational structures including the Incident Command System and the Emergency Support Function structures. Analytic products developed in support of Protection activities during steady state conditions are also designed to support Response planning efforts, and provide the basis for operational planning during incident response. Assessments of infrastructure impacts, and prioritization efforts during response also rely on the structures and	The Recovery and Protection Mission Areas will occur concurrently. Protection does not cease during Recovery. Coordination with the pre- and post-disaster recovery plans will ensure a resilient recovery process that takes protection into account. Protection and mitigation focus on a sustainable economy and community resilience and not just the swift restoration of infrastructure, buildings, and services. Establishing recovery priorities, and ensuring that resilience and risk management are central to the recovery effort, requires the Protection mission to structure its activities in a way that supports Recovery efforts.

Relationship of the Protection Mission Area with the Other Mission Areas				
	Prevention	Mitigation	Response	Recovery
	<p>mission.</p> <p>Prevention and Protection operate simultaneously and to provide for seamless integration when needed. For example, during a period of imminent terrorist threat, Prevention activities may focus on information sharing, law enforcement operations, and other activities to prevent, deter, and preempt terrorism. Protection may assess the increased risks and coordinates the information sharing and other actions needed to enhance specific protective measures.</p>		<p>relationships developed within the Protection mission</p>	

367

368

369 **Appendix 1 to Annex A: Protection Federal Leadership**
370 **Group Charter**

371 Lorem Ipsum. [This section will contain information relating to the composition and conduct of a
372 Protection Federal Leadership Group.]

373

374

DRAFT

375 **Appendix 2 to Annex A: Networked Coordination**

376 Lorem Ipsum [this section will lay out further detailed principles for the inter-organizational
377 coordination model for federal protection activities.]

378

379

380

DRAFT

381 **Annex B: Protection Planning**

382 *Planning*

383 [Lorem Ipsum. This section will outline the manner in which Federal agencies conduct Protection
384 mission planning activity.]

385 **Delivery of Federal Planning to the Mission Area**

- 386 ▪ Provide a flexible Federal planning process that builds on existing plans and facilitates the
387 development of additional plans to Protection stakeholders.
- 388 ▪ Sustain existing and establish new information sharing mechanisms among Protection
389 stakeholders to enable planning/protection of critical infrastructures within jurisdictions.
- 390 ▪ Support the training of State, local, tribal, territorial, private sector, and non-profit planners using
391 approved Federal planning process and current best-practices.
- 392 ▪ Provide standard Federal metrics to facilitate the identification/prioritization of critical
393 infrastructure and determination of risk.
- 394 ▪ Integrate Federal grants to support funding of Protection planning efforts as appropriate.
- 395 ▪ Provide a national vulnerability assessment capability to support vulnerability assessments,
396 perform risk analyses, identify capability gaps, and coordinate protective measures on an ongoing
397 basis in conjunction with the private sector and Federal, state, and local organizations and
398 agencies.
- 399 ▪ Develop and disseminate a series of Federal Protection resilience, and continuity plans and
400 programs to address protection specific requirements.
- 401 ▪ Develop, coordinate, and execute protection related- exercises on a recurring annual basis;
402 Lessons learned will be integrated into plans, policies, and procedures as appropriate.

403 **Federal Planning Critical Tasks**

- 404 ▪ [Critical tasks the Federal government will execute to deliver, synchronize, and integrate the
405 planning cross-cutting core capability]

406 In summary, Federal Departments and Agencies will identify their ability to assess the threat,
407 identify authorities for key decision points, deploy and employ assets and capabilities, and identify
408 requirements and request support, in order to protect people, critical assets, systems, and networks
409 against the greatest risks to the Nation. Planning activities will also identify assumptions to inform
410 decision-making. If necessary, departments and agencies will adjust their operational plans based on
411 direction from the President of the United States. Prior to such direction, departments and agencies
412 will execute their roles and responsibilities pursuant to law, national policy, national plans, and their
413 respective agency plans.

414 *Public Information & Warning*

415 Public information and warning is delivering coordinated, prompt, reliable, and actionable
416 information to the whole community through the use of clear, consistent, accessible, and culturally
417 and linguistically appropriate methods.

418 **Delivery of Public Information and Warning to the Mission Area**

419 The Federal government will develop executable multi-echelon plans to provide whole of community
420 information sharing among all levels of government. This includes, but is not limited to, the
421 following activities:

- 422 ▪ Establish mechanisms and provide the full spectrum of support necessary for appropriate and
423 ongoing information sharing among all levels of government, the private sector,
424 nongovernmental organizations, and the public.
- 425 ▪ Integration of appropriate coordination mechanisms (such as the Integrated Public Alert and
426 Warning System, National Terrorism Advisory System , and social media sites and technology
- 427 ▪ Establish coordination mechanisms that facilitate the rapid exchange of information sharing
428 among stakeholders during steady-state, escalated decision making and response environments.

429 **Federal Public Information and Warning Critical Tasks**

- 430 ▪ [Critical tasks the Federal government will deliver, synchronize, and integrate the public
431 information and warning]

432 **Operational Coordination**

433 Operational coordination is establishing and maintaining unified and coordinated operational
434 structures and processes that appropriately integrate all critical stakeholders and support the
435 execution of core capabilities.

436 **Delivery of Operational Coordination to the Mission Area**

437 [Lorem Ipsum]

438 **Federal Operational Coordination Critical Tasks**

- 439 ▪ [Critical tasks the Federal government will deliver, synchronize, and integrate operational
440 coordination]

441 For Operational Coordination, all Federal departments and agencies will execute their individual
442 authorities as stated in law or guidance. Each department and agency will coordinate their activities
443 through their operations centers through means such as liaisons or reports. The Protection Federal
444 Leadership group will coordinate issues across operational levels to ensure operations across the
445 Federal Government are coordinated for unity of effort.

446

447

448 **Appendix 1 to Annex B: Access Control and Identity**
449 **Verification**

450 [Lorem Ipsum. Core capability appendices will provide greater detail and description of the way that
451 individual core capabilities are developed and coordinated at the Federal level.]

452
453
454

DRAFT

455 **Appendix 2 to Annex B: Intelligence and Information** 456 **Sharing**

457 [Lorem Ipsum. Core capability appendices will provide greater detail and description of the way that
458 individual core capabilities are developed and coordinated at the Federal level.]

459 Intelligence and Information Sharing capabilities involve the effective implementation of the
460 intelligence cycle and information fusion processes by local, state, tribal, territorial, and Federal
461 intelligence entities, the private sector, and the public to develop situational awareness of potential
462 threats and hazards within the United States.

463 **Delivery of Intelligence and Information Sharing to the Mission Area**

464 The Federal government will monitor, gather, and analyze intelligence and information in order to
465 protect people, critical assets, systems, and networks against the greatest risks to the Nation. This
466 includes, but is not limited to:

- 467 ▪ Establish and update national, state, local and regional education awareness programs to facilitate
468 information/intelligence sharing among all Protection stakeholders.
- 469 ▪ Recurring training and exercising of intelligence/information sharing at multiple levels and
470 echelons – integration of lessons learned as appropriate
- 471 ▪ Establish and implementation of routine exchange of security information—including threat
472 assessments, alerts, attack indications and warnings, and advisories—among Protection
473 stakeholders at all levels and echelons.
- 474 ▪ Production and dissemination of relevant, timely, accessible, and actionable intelligence and
475 information products to others as applicable (including ‘tear lines’ to facilitate information
476 sharing)
- 477 ▪ Education of stakeholders on safeguarding and sharing of sensitive and classified information.

478 **Federal Intelligence and Information Sharing Critical Tasks**

479 Critical tasks the Federal government will deliver, synchronize, and integrate the intelligence and
480 information sharing are identified in the figure below.

- 481 ▪ Monitor, detect, and analyze threats and hazards to public safety, health, and security, which
482 include:
- 483 ▪ Participation in local, state, tribal, territorial, regional, and national education and awareness
484 programs.
- 485 ▪ Participation in the routine exchange of security information—including threat assessments,
486 alerts, attack indications and warnings, and advisories—among partners.
- 487 ▪ Determine requirements for Protection stakeholder intelligence, information, and information
488 sharing.
- 489 ▪ Develop or identify and provide access to mechanisms and procedures for intelligence and
490 information sharing between the public, private sector, and government Protection partners.
- 491 ▪ Using intelligence processes, produce and deliver relevant, timely, accessible, and actionable
492 intelligence and information products to others as applicable, to include partners in the other
493 mission areas.

494 Adhere to appropriate mechanisms for safeguarding sensitive and classified information.

495 **Federal Personnel and Resources**

496 [A summary of resources required to deliver this Protection core capability]

497

498

499

DRAFT

500 **Appendix 3 to Annex B: Interdiction and Disruption**

501 [Lorem Ipsum. Core capability appendices will provide greater detail and description of the way that
502 individual core capabilities are developed and coordinated at the Federal level.]

503 Interdiction and disruption is the delaying, diverting, intercepting, halting, apprehending, or securing
504 threats and/or hazards.

505 These threats and hazards include people, materials, or activities that pose a threat to the Nation,
506 including domestic and transnational criminal and terrorist activities and the unlawful movement and
507 acquisition/transfer of chemical, biological, radiological, nuclear, and explosive (CBRNE) materials
508 and related technologies.

509 **Delivery of Interdiction and Disruption to the Mission Area**

510 In the context of Protection this capability includes interdiction and disruption activities conducted
511 by law enforcement and public and private sector security personnel during the course of their
512 routine duties, including the enforcement of border authorities at and between ports of entry into the
513 United States. It might also include urgent activities required when an imminent threat is encountered
514 unexpectedly through the course of day to day protection activities.

515 **Federal Interdiction and Disruption Critical Tasks.**

- 516 ■ [Critical tasks the Federal government will deliver, synchronize, and integrate interdiction and
517 disruption]

518

519

520 **Appendix 4 to Annex B: Screening, Search, and Detection**

521 [Lorem Ipsum. Core capability appendices will provide greater detail and description of the way that
522 individual core capabilities are developed and coordinated at the Federal level.]

523 Identifying, discovering, or locating threats and/or hazards through active and passive surveillance
524 and search procedures. These activities may include the use of systematic examinations and
525 assessments, sensor technologies, disease surveillance, laboratory testing, or physical investigation
526 and intelligence.

527 **Delivery of Screening, Search, and Detection to the Mission Area**

528 The Federal government will apply active and passive surveillance and search procedures to identify,
529 discover, or locate threats or hazards. This includes, but is not limited to:

- 530 ▪ Use of systematic examinations and assessments, sensor technologies, public health disease
531 surveillance, laboratory testing, or physical investigation and intelligence.
- 532 ▪ Employment of personnel and resources to locate persons and criminal/terrorist networks
533 associated with a potential threat.
- 534 ▪ Establishment of integrated national, regional, and local mechanisms to develop and engage an
535 observant Nation (individuals, families, communities, and state and local government and private
536 sector partners).
- 537 ▪ Active integrated screening of persons, baggage, mail, cargo, and conveyances using technical,
538 non-technical, intrusive, and non-intrusive means.
- 539 ▪ Establish training /periodic exercising of all surveillance and search procedures; integration of
540 lessons learned as appropriate.
- 541 ▪ Periodic physical searches within established legal authorities and protocols.
- 542 ▪ Implementation of CBRNE search and detection operations.
- 543 ▪ Conduct ambient and active detection of CBRNE agents.
- 544 ▪ Operate safely in a hazardous environment.
- 545 ▪ Conduct technical search and detection operations.
- 546 ▪ Consider deployment of Federal teams and capabilities to enhance capabilities to enhance state
547 and local efforts, including use of incident assessment and awareness assets.
- 548 ▪ Establish nation-wide CBRNE surveillance of health threats and hazards
- 549 ▪ Integrate Federal grant programs to support programs and initiatives

550 **Federal Screening, Search, and Detection Critical Tasks**

551 Federal government actions to deliver synchronize and integrate intelligence and information sharing
552 functions.

- 553 ▪ [Critical tasks the Federal government will deliver, synchronize, and integrate screening, search,
554 and detection]

555
556

557 **Appendix 5 to Annex B: Physical Protective Measures**

558 [Lorem Ipsum. Core capability appendices will provide greater detail and description of the way that
559 individual core capabilities are developed and coordinated at the Federal level.]

560

561

DRAFT

562 **Appendix 6 to Annex B: Risk Management for Protection**
563 **Programs and Activities**

564 [Lorem Ipsum. Core capability appendices will provide greater detail and description of the way that
565 individual core capabilities are developed and coordinated at the Federal level.]

566

567

DRAFT

568 **Appendix 7 to Annex B: Cybersecurity**

569 [Lorem Ipsum. Core capability appendices will provide greater detail and description of the way that
570 individual core capabilities are developed and coordinated at the Federal level.]

571

572

DRAFT

573 **Appendix 8 to Annex B: Supply Chain Integrity and**
574 **Security**

575 [Lorem Ipsum. Core capability appendices will provide greater detail and description of the way that
576 individual core capabilities are developed and coordinated at the Federal level.]

577

578

DRAFT

579 **Annex C: Coordinating Activities**

580 This annex provides a summary of the concept, plans, arrangements and key authorities that
581 coordinate protection mission activity across ten major areas. As described in the base plan the
582 protection mission activities addressed in this FIOP are not an exhaustive or exclusive list. As
583 Protection concerns emerge, the mission adapts and evolves to address them. The ten coordinating
584 activities described in this FIOP are existing means of coordinating Protection activity within distinct
585 and established domains of operation:

- 586 ▪ **Border Security.** Securing U.S. air, land, and sea ports and borders against the illegal flow of
587 people and goods, while facilitating the flow of lawful travel and commerce.
- 588 ▪ **Critical Infrastructure Protection.** Protecting the physical and cyber elements of critical
589 infrastructure. This includes actions to deter the threat, reduce vulnerabilities, or minimize the
590 consequences associated with a terrorist attack, natural disaster, or manmade disaster. Critical
591 Infrastructure Protection is an element of critical infrastructure security and resilience as detailed
592 in Presidential Policy Directive 21: Critical Infrastructure Security and Resilience.¹³
- 593 ▪ **Cybersecurity.** Securing the cyber environment and infrastructure from unauthorized or
594 malicious access, use, or exploitation while protecting privacy, civil rights, and other civil
595 liberties.
- 596 ▪ **Defense Against Weapons of Mass Destruction (WMD) Threats.** Protecting the Nation from
597 threats associated with WMD and related materials and technologies including their malicious
598 acquisition, movement, and use within the United States.
- 599 ▪ **Defense of Agriculture and Food.** Defending agriculture and food networks and systems from
600 all-hazards threats and incidents.¹⁴

¹³ Critical infrastructure, as defined in PPD-21, includes those systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security; economy; public safety or health; environment; or any combination of these matters, across any jurisdiction. Critical infrastructure security and resilience addresses sectors along common functions that include chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

¹⁴ Core capabilities for Protection align with policy established in HSPD 9: Defense of United States Agriculture and Food to include identifying and prioritizing sector critical infrastructure; developing awareness and early warning capabilities; mitigating vulnerabilities; and enhancing screening procedures.

- 601 ▪ **Health Security.** Securing the Nation and its people to be prepared for, protected from, and
602 resilient in the face of health threats or incidents with potentially negative health consequences.
- 603 ▪ **Immigration Security.** Securing the Nation from illegal immigration through effective and
604 efficient immigration systems and processes that respect human and civil rights.
- 605 ▪ **Maritime Security.** Securing U.S. maritime infrastructure, resources, and the Marine
606 Transportation System from terrorism and other threats and hazards and securing the homeland
607 from an attack from the sea, while preserving civil rights, respecting privacy and protected civil
608 liberties, and enabling legitimate travelers and goods to move efficiently without fear of harm or
609 significant disruption.
- 610 ▪ **Protection of Key Leadership and Events.** Safeguarding government executive leadership from
611 hostile acts by terrorists and other malicious actors and to ensure security at events of national
612 significance.¹⁵
- 613 ▪ **Transportation Security.** Securing U.S. transportation systems and the air domain against
614 terrorism and other threats and hazards, while preserving civil rights, respecting privacy and
615 protected civil liberties, and enabling legitimate travelers and goods to move without fear of harm
616 or significant disruption.
- 617
- 618
- 619

¹⁵ 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 (NSSE) as defined in Title 18, U.S.C. Section 3056 and further clarified in PPD-22, and events assessed under the Special Event Assessment Rating (SEAR) process by the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) based on input from Federal, state, and local law enforcement entities.

620 **Appendix 1 to Annex C: Border Security**

621 Lorem Ipsum (mission activity introduction and summary)

622 **Concept of Operations**

623 Lorem Ipsum

624 **Coordination Structures**

625 Lorem Ipsum

626 **Existing Plans etc.**

627 Lorem Ipsum

628 **Key Authorities and References.**

629 The following laws, policy directives, strategies, plans, and executive orders are included in addition
630 to the general authorities/references provided in the base plan for the Border Security Mission
631 Activity.

- 632 ▪ National Southwest Border Counternarcotics Strategy (June 2009)
- 633 ▪ The National Security Strategy, May 2010.
- 634 ▪ The Partnership for 21st Century U.S. Southwest Border Security, April 2010.
- 635 ▪ National Northern Border Counter Drug Strategy
- 636 ▪ The 2010 National Drug Control Strategy.
- 637 ▪ The Quadrennial Homeland Security Review (QHSR), February 2014.
- 638 ▪ The Quadrennial Defense Review (QDR), February 2010.
- 639 ▪ The National Interdiction Command and Control Plan (NICCP), March 2010.
- 640 ▪ The Department of Justice Strategy for Combating Mexican Cartels, November 2009.
- 641 ▪ The Maritime Operations Coordination Plan (MOC-P)

642 **Other.**

643 ▪

644

645

646

647 **Appendix 2 to Annex C: Critical Infrastructure Protection**

648 The Federal Government capability to secure the nation’s critical infrastructure against acts of
649 terrorism and manmade or natural disasters is comprised of critical infrastructure protection activities
650 that promote security by reducing the likelihood of incidents occurring, and enhance resilience by
651 reducing the impact and/or duration of disruptive events on critical infrastructure. The effectiveness
652 of these activities rely upon the close coordination and alignment of practices and functional
653 relationships across the Federal Government including partnerships with State, local, tribal and
654 territorial (SLTT) entities, and critical infrastructure partners (including owners and operators). The
655 National Infrastructure Protection Plan (NIPP) – *NIPP 2013: Partnering for Critical Infrastructure*
656 *Security and Resilience* – outlines how government and private sector participants in the critical
657 infrastructure community work together to manage risks and achieve security and resilience
658 outcomes. The NIPP builds upon the critical infrastructure risk management framework of previous
659 versions of the NIPP and establishes a vision, mission, and goals that are supported by a set of core
660 tenets focused on risk management and partnership to influence future critical infrastructure security
661 and resilience planning at the international, national, regional, SLTT, and owner and operator levels.
662 The NIPP 2013 recognizes the overarching concepts relevant to all critical infrastructure sectors and
663 addresses the physical, cyber, and human considerations required for effective implementation of
664 comprehensive programs. The NIPP 2013 includes a “Call to Action,” which guides the collaborative
665 efforts of the critical infrastructure community to advance security and resilience under three broad
666 activity categories: building upon partnership efforts, innovating in managing risk, and focusing on
667 outcomes. The NIPP 2013 also includes the overarching framework for a structured partnership
668 approach between the government and private sector for protection, security, and resilience of critical
669 infrastructure. It establishes the mechanisms for collaboration between private sector owners and
670 operators and government agencies as well as the requirements for partnerships between the Federal
671 Government; critical infrastructure owners and operators, and SLTT government entities. The
672 sections below outline Federal Government roles responsibilities within the NIPP partnerships in
673 pursuit of critical infrastructure protection activities.

674 **Concept of Operations**

675 Title II of the Homeland Security act of 2002 (as amended) details DHS’s responsibilities as lead
676 agency for critical infrastructure protection. Pursuant to Presidential Policy Directive – 21: Critical
677 Infrastructure Security and Resilience (PPD-21), because each critical infrastructure sector has
678 unique characteristics, operating models, and risk profiles, Sector-Specific Agencies (SSA) that have
679 institutional knowledge and specialized expertise about each sector have been identified.
680 Descriptions of lead and SSA roles and responsibilities are below.

681 **Lead Agency**

682 The Secretary of Homeland Security provides strategic guidance, promotes a national unity of effort,
683 and coordinates the overall Federal effort to promote the security and resilience of the Nation’s
684 critical infrastructure. DHS’s responsibilities as SSA or co-SSA for multiple sectors are described in
685 the SSAs sections below. In carrying out the responsibilities of the Homeland Security Act of 2002,
686 as amended, the Secretary of Homeland Security:

- 687 ■ Evaluates national capabilities, opportunities, and challenges in securing and making resilient
688 critical infrastructure;
- 689 ■ Analyzes threats to, vulnerabilities of, and potential consequences from all hazards on critical
690 infrastructure;

- 691 ■ Identifies security and resilience functions that are necessary for effective public-private
692 engagement with all critical infrastructure sectors;
- 693 ■ Develops a national plan and metrics, in coordination with SSAs and other critical infrastructure
694 partners;
- 695 ■ Integrates and coordinates Federal cross-sector security and resilience activities;
- 696 ■ Identifies and analyzes key interdependencies among critical infrastructure sectors; and
- 697 ■ Reports on the effectiveness of national efforts to strengthen the Nation's security and resilience
698 posture for critical infrastructure.

699 DHS contains a cyber and physical critical infrastructure function that coordinates the effort to
700 protect and enhance the resilience of the nation's physical and cyber infrastructure as well as execute
701 responsibilities as the SSA for multiple sectors as described in the SSA sections below. This function
702 also contains the designated national cyber and physical critical infrastructure centers as described
703 below. The cyber and physical critical infrastructure function responsibilities include:

- 704 ■ Providing situational awareness of critical infrastructure protection issues and activities by
 - 705 ● Developing and analyzing information, including:
 - 706 ○ Incident reporting, open source reporting, field reports and assessments
 - 707 ○ Modeling and simulation
 - 708 ○ .gov domain monitoring
 - 709 ○ Dynamic prioritization of infrastructure
 - 710 ○ Risk analysis
 - 711 ● Sharing information across the government and private sector, including:
 - 712 ○ Data integration and visualization
 - 713 ○ Information exchange on threats and hazards
- 714 ■ Identifying and enabling risk mitigation and reduction through:
 - 715 ● Partnerships and capacity building:
 - 716 ○ Working with critical infrastructure owners and operators in the field and at the national
717 level to identify risks and promote best practices
 - 718 ○ Guiding the national unity of effort for critical infrastructure and resilience
 - 719 ○ Providing technical assistance to build capacity and mitigate risks
 - 720 ● Conducting and supporting assessments:
 - 721 ○ Conducting and supporting vulnerability and consequence assessments, including
722 infrastructure sector-specific assessments, key asset assessments, and regional
723 assessments
 - 724 ○ Conducting Federal facility assessments
- 725 ■ Protecting physical and cyber infrastructure through:
 - 726 ● Security and law enforcement services:

- 727 ○ Federal network security
- 728 ○ Protecting government assets, systems, and networks (physical, virtual, and human)
- 729 ○ Regulating highest risk chemical facilities and ammonium nitrate sales
- 730 ● Incident management coordination:
 - 731 ○ Cybersecurity
 - 732 ○ Physical incident response support
 - 733 ○ Analytic support

734 ***National Infrastructure Coordinating Center***

735 The National Infrastructure Coordinating Center (NICC) is an operational component of NPPD, and
736 the national physical infrastructure center as designated by the Secretary of Homeland Security. The
737 NICC coordinates a national network dedicated to the security and resilience of the critical
738 infrastructure of the United States by providing 24/7 situational awareness, information sharing, and
739 fostering a unity of effort. Establishing and maintaining relationships with critical infrastructure
740 partners both within and outside the Federal government is at the core of the NICC's ability to
741 execute its functions. The NICC collaborates with Federal departments and agencies and private
742 sector partners to monitor potential, developing, and current regional and national operations of the
743 Nation's critical infrastructure sectors.

744 ***National Cybersecurity and Communications Integration Center***

745 The National Cybersecurity and Communications Integration Center (NCCIC) is the cyber
746 operational component of NPPD and is the national cyber critical infrastructure center designated by
747 and the Secretary of Homeland Security. The NCCIC secures federal civilian agencies in cyberspace;
748 provides support and expertise to private sector partners and SLTT entities; and coordinates with
749 international partners. The NCCIC also coordinates the Federal Government protection, mitigation,
750 response, and recovery efforts for significant cyber and communications incidents affecting critical
751 infrastructure in accordance with PPD-21.

752 ***Sector-Specific Agencies***

753 Each critical infrastructure sector has unique characteristics, operating models, and risk profiles. The
754 Federal SSA or co-SSA assigned to each sector has institutional knowledge and specialized expertise
755 about their sector(s). Recognizing existing statutory or regulatory authorities of specific Federal
756 departments and agencies, and leveraging existing sector familiarity and relationships, SSAs:

- 757 ■ Coordinate with DHS and other relevant Federal departments and agencies and collaborate with
758 critical infrastructure owners and operators, where appropriate with independent regulatory
759 agencies, and with SLTT entities, as appropriate;
- 760 ■ Serve as a day-to-day Federal interface for the dynamic prioritization and coordination of critical
761 infrastructure sector-specific activities;
- 762 ■ Carry out critical infrastructure incident management responsibilities consistent with statutory
763 authority and other appropriate policies, directives, or regulations;
- 764 ■ Provide, support, or facilitate technical assistance and consultations for that sector to identify
765 vulnerabilities and help mitigate incidents, as appropriate; and

- 766 ▪ Support the Secretary of Homeland Security’s statutorily required reporting requirements by
767 providing, on an annual basis, sector-specific critical infrastructure information.

768 Each critical infrastructure sector maintains a Sector-Specific Plan which details how the National
769 Infrastructure Protection Plan’s risk management framework is implemented within the sector’s
770 unique characteristics and risk landscape. Each Sector-Specific Agency develops a sector-specific
771 plan through a coordinated effort involving its public and private sector partners.

772 ***Chemical Sector (DHS)***

773 The Chemical Sector can be divided into five main segments, based on the end product produced:
774 basic chemicals, specialty chemicals, agricultural chemicals, pharmaceuticals, and consumer
775 products. Each of these segments has distinct characteristics, growth dynamics, markets, new
776 developments, and issues. Because the majority of Chemical Sector facilities are privately owned,
777 DHS builds stakeholder capacity and enhances critical infrastructure security and resilience through
778 voluntary partnerships that provide training, resources, and exercises. DHS has also issued regulatory
779 Chemical Facility Anti-Terrorism Standards (CFATS) for any facility that manufactures, uses, stores,
780 or distributes certain chemicals at or above specified quantities or concentrations. DHS is designated
781 as the SSA for the Chemical Sector.

782 ***Commercial Facilities Sector (DHS)***

783 Facilities associated with the Commercial Facilities Sector operate on the principle of open public
784 access, meaning that the general public can move freely throughout these facilities without the
785 deterrent of highly visible security barriers. The Commercial Facilities Sector consists of eight
786 subsectors: Public Assembly (e.g., arenas, stadiums, aquariums, zoos, museums, convention centers),
787 Sports Leagues (e.g., professional sports leagues and federations), Gaming (e.g., casinos), Lodging
788 (e.g., hotels, motels, conference centers), Outdoor Events (e.g., theme and amusement parks, fairs,
789 campgrounds, parades), Entertainment and Media (e.g., motion picture studios, broadcast media),
790 Real Estate (e.g., office and apartment buildings, condominiums, mixed use facilities, self-storage),
791 Retail (e.g., retail centers and districts, shopping malls). DHS is designated as the SSA for the
792 Commercial Facilities Sector.

793 ***Communications Sector (DHS)***

794 PPD-21 identifies the Communications Sector as critical because it provides an “enabling function”
795 across all critical infrastructure sectors. Over the last 25 years, the sector has evolved from
796 predominantly a provider of voice services into a diverse, competitive, and interconnected industry
797 using terrestrial, satellite, and wireless transmission systems. The transmission of these services has
798 become interconnected; satellite, wireless, and wireline providers depend on each other to carry and
799 terminate their traffic and companies routinely share facilities and technology to ensure
800 interoperability. DHS is the SSA for the Communications Sector.

801 ***Critical Manufacturing Sector (DHS)***

802 The Critical Manufacturing Sector identified the following industries to serve as the core of the
803 sector: primary metal manufacturing; machinery manufacturing; electrical equipment, appliance, and
804 component manufacturing; and transportation equipment manufacturing. Products made by these
805 manufacturing industries are essential to many other critical infrastructure sectors. DHS is designated
806 as the SSA for the Critical Manufacturing Sector.

807 Dams Sector (DHS)

808 The Dams Sector is composed of assets that include dam projects, hydropower generation facilities,
809 navigation locks, levees, dikes, hurricane barriers, mine tailings, other industrial waste
810 impoundments, and other similar water retention and water control facilities. The Dams Sector is a
811 vital part of the nation’s infrastructure and provides a wide range of economic, environmental, and
812 social benefits, including hydroelectric power, river navigation, water supply, wildlife habitat, waste
813 management, flood control, and recreation. The Dams Sector has interdependencies with a wide
814 range of other sectors. DHS is designated as the SSA for the Dams Sector.

815 Defense Industrial Base Sector (Department of Defense (DOD))

816 The Defense Industrial Base Sector is the worldwide industrial complex that enables research and
817 development, as well as design, production, delivery, and maintenance of military weapons systems,
818 subsystems, and components or parts, to meet U.S. military requirements. The Defense Industrial
819 Base partnership consists of Department of Defense components, Defense Industrial Base companies
820 and their subcontractors who perform under contract to the Department of Defense, companies
821 providing incidental materials and services to the Department of Defense, and government-
822 owned/contractor-operated and government-owned/government-operated facilities. Defense
823 Industrial Base companies include domestic and foreign entities, with production assets located in
824 many countries. The sector provides products and services that are essential to mobilize, deploy, and
825 sustain military operations. The Defense Industrial Base Sector does not include the commercial
826 infrastructure of providers of services such as power, communications, transportation, or utilities that
827 the Department of Defense uses to meet military operational requirements. These commercial
828 infrastructure assets are addressed by other SSAs. The Department of Defense is designated as the
829 SSA for the Defense Industrial Base Sector.

830 Emergency Services Sector (DHS)

831 A system of prevention, preparedness, response, and recovery elements, the Emergency Services
832 Sector (ESS) represents the nation’s first line of defense in the prevention and mitigation of risk from
833 both intentional and unintentional manmade incidents, as well as from natural disasters. The majority
834 of ESS functions are performed at the state, local, tribal, and territorial levels, and are defined by five
835 disciplines: Law Enforcement; Fire and Emergency Services; Emergency Management; Emergency
836 Medical Services; Public Works. Additionally, there are several specialized capabilities identified
837 within the ESS, such as: Hazardous Materials; Search and Rescue; Explosive Ordnance Disposal
838 (i.e., bomb squads); Tactical Operations (i.e., SWAT); Aviation Units (i.e., police and medevac
839 helicopters); Public Safety Answering Points (i.e., 9-1-1 call centers). DHS is designated as the SSA
840 for the ESS.

841 Energy Sector (Department of Energy)

842 Energy infrastructure is divided into three interrelated segments, including: electricity, petroleum,
843 and natural gas. The heavy reliance on pipelines to distribute products across the nation highlights
844 the interdependencies between the Energy and Transportation Systems Sector. The reliance of
845 virtually all industries on electric power and fuels means that all sectors have some dependence on
846 the Energy Sector. PPD-21 identifies the Energy Sector as uniquely critical because it provides an
847 “enabling function” across all critical infrastructure sectors. More than 80 percent of the country’s
848 energy infrastructure is owned by the private sector, supplying fuels to the transportation industry,
849 electricity to households and businesses, and other sources of energy that are integral to growth and
850 production across the nation. The Department of Energy is designated as the SSA for the Energy
851 Sector.

852 ***Financial Services Sector (Treasury)***

853 Within the Financial Services Sector, financial institutions are organized and regulated based on
854 services provided by institutions. Within the sector, there are more than 18,800 federally insured
855 depository institutions; thousands of providers of various investment products, including roughly
856 18,440 broker-dealer, investment adviser, and investment company complexes; providers of risk
857 transfer products, including 7,948 domestic U.S. insurers; and many thousands of other credit and
858 financing organizations. The Department of Treasury is designated as the SSA for the Financial
859 Services Sector.

860 ***Food and Agriculture Sector (Health and Human Services (HHS) and U.S. Department of***
861 ***Agriculture (USDA))***

862 The Food and Agriculture Sector is almost entirely under private ownership and is composed of an
863 estimated 2.2 million farms, 900,000 restaurants, and more than 400,000 registered food
864 manufacturing, processing, and storage facilities. This sector accounts for roughly one-fifth of the
865 nation's economic activity. The Food and Agriculture Sector has critical dependencies with many
866 sectors, but particularly with the following: Water and Wastewater Systems, for clean irrigation and
867 processed water; Transportation Systems, for movement of products and livestock; Energy, to power
868 the equipment needed for agriculture production and food processing; and Financial Services,
869 Chemical, and Dams. The Department of Agriculture and the Department of Health and Human
870 Services are designated as the Co-SSAs for the Food and Agriculture Sector.

871 More information on protection activities in the Food and Agriculture Sector is contained in
872 Appendix 5: Defense of Agriculture and Food Activities.

873 ***Government Facilities Sector (DHS and General Services Administration)***

874 The Government Facilities Sector includes a wide variety of buildings, located in the United States
875 and overseas, that are owned or leased by Federal, state, local, and tribal governments. Many
876 government facilities are open to the public for business activities, commercial transactions, or
877 recreational activities while others that are not open to the public contain highly sensitive
878 information, materials, processes, and equipment. In addition to physical structures, the sector
879 includes cyber elements that contribute to the protection of sector assets (e.g., access control systems
880 and closed-circuit television systems) as well as individuals who perform essential functions or
881 possess tactical, operational, or strategic knowledge.

882 The Education Facilities Subsector covers pre-kindergarten through 12th grade schools, institutions of
883 higher education, and business and trade schools. The subsector includes facilities that are owned by
884 both government and private sector entities. The National Monuments and Icons Subsector
885 encompasses a diverse array of assets, networks, systems, and functions located throughout the
886 United States. Many National Monuments and Icons assets are listed in either the National Register
887 of Historic Places or the List of National Historic Landmarks. DHS and the General Services
888 Administration are designated as the Co-SSAs for the Government Facilities Sector.

889 ***Healthcare and Public Health Sector (HHS)***

890 The Healthcare and Public Health Sector protects all sectors of the economy from hazards including
891 infectious disease outbreaks. Operating in all U.S. states, territories, and tribal areas, the sector plays
892 a significant role in response and recovery across all other sectors in the event of a natural or
893 manmade disaster. While healthcare tends to be delivered and managed locally, the public health
894 component of the sector, focused primarily on population health, is managed across all levels of
895 government: national, state, regional, local, tribal, and territorial. The Healthcare and Public Health

896 Sector is highly dependent on fellow sectors for continuity of operations and service delivery,
897 including: Communications, Emergency Services, Energy, Food and Agriculture, Information
898 Technology, Transportation Systems, and Water and Wastewater Systems. The Department of Health
899 and Human Services is designated as the SSA for the Healthcare and Public Health Sector.

900 More information on protection activities in the Healthcare and Public Health Sector is contained in
901 Appendix 6: Health Security.

902 ***Information Technology Sector (DHS)***

903 The Information Technology Sector is central to the nation's security, economy, and public health
904 and safety. The Information Technology's virtual and distributed functions produce and provide
905 hardware, software, and information technology systems and services, and – in collaboration with the
906 Communications Sector – the Internet. Although information technology infrastructure has a certain
907 level of inherent resilience, its interdependent and interconnected structure presents challenges as
908 well as opportunities for coordinating public and private sector preparedness and protection
909 activities. DHS is designated as the SSA for the Information Technology Sector.

910 More information on protection activities in the Information Technology Sector is contained in
911 Appendix 3: Cybersecurity.

912 ***Nuclear Reactors, Materials, and Waste Sector (DHS)***

913 Nuclear power accounts for approximately 20 percent of our nation's electrical generation, provided
914 by 100 commercial nuclear reactors licensed to operate at 62 nuclear power plants. The sector
915 includes: nuclear power plants; non-power nuclear reactors used for research, testing, and training;
916 manufacturers of nuclear reactors or components; radioactive materials used primarily in medical,
917 industrial, and academic settings; nuclear fuel cycle facilities; decommissioned nuclear power
918 reactors; and transportation, storage, and disposal of nuclear and radioactive waste. The sector is
919 interdependent with other critical infrastructure sectors: Chemical Sector, as a consumer of chemicals
920 through the nuclear fuel cycle and at reactor sites; Energy Sector, as a supplier of electricity to our
921 nation's electrical grid; Healthcare and Public Health Sector, as a supplier of nuclear medicine,
922 radiopharmaceuticals, and in the sterilization of blood and surgical supplies; and the Transportation
923 Systems Sector, through the movement of radioactive materials. DHS is designated as the SSA for
924 the Nuclear Reactors, Materials, and Waste Sector.

925 ***Transportation Systems Sector (DHS and Department of Transportation)***

926 The Transportation Systems Sector consists of seven key subsectors, or modes: aviation (including
927 aircraft, air traffic control systems, and commercial and other airports, heliports, and landing strips
928 (including those for civil and joint use with the military); highway infrastructure and motor carrier
929 (including roadways, bridges, and tunnels; as well as vehicles [automobiles, motorcycles, trucks,
930 commercial freight vehicles, motorcoaches, and school buses]); maritime transportation system
931 (coastline, ports, waterways, Exclusive Economic Zone, and intermodal landside connections); mass
932 transit and passenger rail (service by buses, rail transit, long-distance rail, cable cars, inclined planes,
933 funiculars, and automated guideway systems); pipeline systems (carrying natural gas, hazardous
934 liquids, and chemicals, including liquefied natural gas processing and storage facilities); freight rail
935 (including major carriers, small railroads, active railroad, freight cars, and locomotives [also includes
936 track and structures DOD-designated as critical to mobilization and resupply of U.S. forces]); and
937 postal and shipping (differentiated by general cargo operations). DHS and the Department of
938 Transportation are designated as the Co-Sector-Specific Agencies for the Transportation Systems
939 Sector.

940 More information on protection activities in the Transportation Sector is contained in Appendix 10:
941 Transportation Security.

942 ***Water and Wastewater Systems Sector (Environmental Protection Agency)***

943 The Water and Wastewater Systems Sector includes public drinking water systems and wastewater
944 treatment systems in the United States. The vast majority of the U.S. population receives their
945 potable water from these drinking water systems, and has its sanitary sewerage treated by these
946 wastewater systems. The Water and Wastewater Systems Sector is vulnerable to a variety of attacks,
947 including contamination with deadly agents, physical attacks such as the release of toxic gaseous
948 chemicals and cyber attacks. Critical sectors such ESS, Healthcare and Public Health, Energy, Food
949 and Agriculture, and Transportation Systems, would suffer negative impacts from a denial of service
950 in the Water and Wastewater Systems Sector. The Environmental Protection Agency is designated as
951 the SSA for the Water and Wastewater Systems Sector.

952 **Coordination Structure**

953 The mechanisms for collaboration between private sector owners and operators and government
954 agencies is outlined in the National Infrastructure Protection Plan (NIPP 2013): Partnering for
955 Critical Infrastructure Security and Resilience which includes the protocols to be used to synchronize
956 communication and actions within the Federal Government and the identified functional relationships
957 within DHS and across the Federal Government including the public-private partnership model.

958 Within this partnership model, Federal Government coordination occurs within Government
959 Coordinating Councils (GCC) the SSAs (as described above), and the Federal Senior Leadership
960 Council (FSLC).

Sector and Cross-Sector Coordinating Structures

Critical Infrastructure Sector	Sector-Specific Agency	Critical Infrastructure Partnership Advisory Council		
		Sector Coordinating Councils (SCCs)	Government Coordinating Councils (GCCs)	Regional Consortia
Chemical	Department of Homeland Security	✓	✓	
Commercial Facilities i		✓	✓	
Communications i		✓	✓	
Critical Manufacturing		✓	✓	
Dams		✓	✓	
Emergency Services i		✓	✓	
Information Technology i		✓	✓	
Nuclear Reactors, Materials & Waste		✓	✓	
Food & Agriculture	Department of Agriculture, Department of Health and Human Services	✓	✓	
Defense Industrial Base i	Department of Defense	✓	✓	
Energy i	Department of Energy	✓	✓	
Healthcare & Public Health i	Department of Health and Human Services	✓	✓	
Financial Services i	Department of the Treasury	Uses separate coordinating entity	✓	
Water & Wastewater Systems i	Environmental Protection Agency	✓	✓	
Government Facilities	Department of Homeland Security, General Services Administration	Sector does not have an SCC	✓	
Transportation Systems i	Department of Homeland Security, Department of Transportation	Various SCCs are broken down by transportation mode or subsector.	✓	

i Indicates that a sector (or a subsector within the sector) has a designated information-sharing organization.

961

962

Figure 5

963 **Government Coordinating Councils**

964 The GCCs enable interagency, intergovernmental, and cross-jurisdictional coordination within and
965 across sectors. They comprise representatives not only from the Federal government, but also SLTT
966 entities (as appropriate to the operating landscape of each individual sector). Each GCC is chaired by
967 a representative from the designated SSA with responsibility for ensuring appropriate representation
968 on the council and providing cross-sector coordination with SLTT governments. The GCC
969 coordinates strategies, activities, policies, and communications across governmental entities within
970 each sector.

971 **Federal Senior Leadership Council**

972 The FSLC is composed of senior officials from the designated SSAs and other Federal departments
973 and agencies identified in PPD-21. The FSLC facilitates enhanced Federal communication and
974 coordination across the sectors focused on critical infrastructure security and resilience.

975 **Connection to other Mission Areas**

976 Within the context of critical infrastructure protection, prevention activities are most closely
977 associated with efforts to address threats; protection efforts generally address vulnerabilities; and
978 response and recovery efforts help minimize consequences. Mitigation efforts transcend the entire
979 threat, vulnerability, and consequence spectrum. To support efforts in advance of or during an
980 incident, the Federal Government critical infrastructure community collaborates based on the
981 structures established in each of the National Planning Frameworks and FIOPs. Specific to the
982 Response preparedness mission area, the Secretary of Homeland Security is the principal Federal
983 official for domestic incident management and coordinates Federal Government responses to
984 significant cyber or physical incidents affecting critical infrastructure (consistent with statutory
985 authorities).¹⁶

986 **Key Plans**

- 987 ■ National Infrastructure Protection Plan (2013) – NIPP 2013: Partnering for Critical Infrastructure
988 Security and Resilience
- 989 ■ Sector-Specific Plans
 - 990 ● Chemical
 - 991 ● Commercial Facilities

¹⁶ These roles of the Secretary related to domestic incident management and preparedness coordination do not interfere with the authority of the Attorney General or Director of the Federal Bureau of Investigation as described in PPD-8 and PPD-21.

- 992 • Communications
- 993 • Critical Manufacturing
- 994 • Dams
- 995 • Defense Industrial Base
- 996 • Emergency Services
- 997 • Energy
- 998 • Financial Services
- 999 • Food and Agriculture
- 1000 • Government Facilities
- 1001 • Healthcare and Public Health
- 1002 • Information Technology
- 1003 • Nuclear Reactors, Materials, and Waste
- 1004 • Transportations Systems
- 1005 • Water and Wastewater Systems

1006 **Key Authorities and References**

1007 The following laws, policy directives, strategies, and executive orders are included in addition to the
1008 general authorities/references provided in the base plan for the Critical Infrastructure Protection
1009 Mission Activity

- 1010 ▪ Title II of the Homeland Security Act of 2002 (Public Law 107–296), as amended, March 2006
- 1011 ▪ Critical Infrastructure Information (CII) Act of 2002
- 1012 ▪ 6 Code of Federal Regulations (CFR) 29, “Procedures for Handling Critical Infrastructure
1013 Information”, September 2006
- 1014 ▪ PPD–17, Countering Improvised Explosive Devices, June 2012
- 1015 ▪ PPD–21, Critical Infrastructure Security and Resilience, February 2013
- 1016 ▪ HSPD–5, Management of Domestic Incidents, February 2003
- 1017 ▪ HSPD–9, Defense of United States Agriculture and Food, January 2004
- 1018 ▪ Executive Order (EO) 12977, Interagency Security Committee, October 1995
- 1019 ▪ EO 13636, Improving Critical Infrastructure Cybersecurity, February 2013
- 1020 ▪ EO 13650, Improving Chemical Facility Safety and Security, August 2013
- 1021 ▪ DHS Fiscal Years 2014-2018 Strategic Plan
- 1022 ▪ The National Protection and Programs Directorate Strategic Plan for Fiscal Years 2014– 2018,
1023 May 2013
- 1024 ▪ National Protection and Programs Directorate Office of Infrastructure Protection Strategic Plan:
1025 2012–2016, August 2012

- 1026 ▪ 2014 Quadrennial Homeland Security Review, June 2014
- 1027 ▪ National Strategy for the Physical Protection of Critical Infrastructures
1028 and Key Assets, February 2003
- 1029 ▪ Critical Infrastructure and Key Resources Support Annex to the National Response Framework,
1030 May 2013
- 1031 ▪ DHS 17001 Delegation to the Under Secretary For National Protection and Programs, October
1032 2013
- 1033 ▪ DHS 17008 Delegation to the Under Secretary For National Protection and Programs Regarding
1034 Chemical Facility Anti-Terrorism Standards, May 2015
- 1035 ▪ SC §1315, Law enforcement authority of Secretary of Homeland Security for protection of public
1036 property, January 2012
- 1037 ▪ Federal Protective Service Policy Directive 15.1.2.1, Law Enforcement Authorities and Powers,
1038 November 2011.
- 1039 Sector Annual Reports (multiple years) – for all sectors, as identified above
- 1040
- 1041
- 1042

1043 **Appendix 3 to Annex C: Cybersecurity**

1044 **Key Authorities and References.**

1045 The following laws, policy directives, strategies, plans, and executive orders are included in addition
1046 to the general authorities/references provided in the base plan for the Cybersecurity Mission Activity:

- 1047 ▪ HSPD-7: Critical Infrastructure Identification, Prioritization, and Protection (2003)
- 1048 ▪ National Strategy to Secure Cyberspace (February 2003)
- 1049 ▪ DHS Quadrennial Homeland Security Review (QHSR) Report (February 1, 2010)
- 1050 ▪ Federal Information Security Management Act of 2002 (FISMA)
- 1051 ▪ National Security Policy Directive-54/ HSPD-23
- 1052 ▪ U.S.C. TITLE 18-Crimes and Criminal Procedure
- 1053 ▪ U.S.C. TITLE 28-Judiciary and Judicial Procedure
- 1054 ▪ U.S.C. TITLE 50-War and National Defense
- 1055 ▪ Executive Order 12333--United States Intelligence Activities
- 1056 ▪ International Strategy for Cyberspace (May 2011)
- 1057 ▪ Department of Defense Strategy for Operating in Cyberspace (July 2011)
- 1058 ▪ National Strategy for Trusted Identities in Cyberspace (April 2011)
- 1059 ▪ The Comprehensive National Cybersecurity Initiative (CNCI)

1060 **Other**

- 1061 ▪

1062

1063

1064 **Appendix 4 to Annex C: Defense Against Weapons of**
1065 **Mass Destruction (WMD) Threats**

1066 **Key Authorities and References.**

1067 The following laws, policy directives, strategies, plans, and executive orders are included in addition
1068 to the general authorities/references provided in the base plan for the Defense Against WMD Threats
1069 Mission Activity.

- 1070 ▪ DHS Nuclear Personnel Reliability Program
- 1071 ▪ Global Threat Reduction Initiative
- 1072 ▪ HSPD-14/National Security Presidential Directive (NSPD)-43
- 1073 ▪ Executive Order 12333
- 1074 ▪ NSPD-54/HSPD-23: Cyber Security and Monitoring
- 1075 ▪ NSPD-46/HSPD-15: U.S. Strategy and Policy in the War on Terror
- 1076 ▪ NSPD-38: National Strategy to Secure Cyberspace
- 1077 ▪ International Atomic Energy Agency (IAEA) Nuclear Security Recommendations on Nuclear
1078 and Other Radioactive Materials out of Regulatory Control (IAEA Nuclear Security Series No.
1079 15)
- 1080 ▪ Global Initiative to Combat Nuclear Terrorism Model Guidelines Document for Nuclear
1081 Detection Architectures (2009)
- 1082 ▪ Global Nuclear Detection Architecture (GNDA) Strategic Plan (2010)
- 1083 ▪ GNDA Annual Report (2011)
- 1084 ▪ National Response Framework (NRF)
- 1085 ▪ Quadrennial Defense Review (QDR) (2010)
- 1086 ▪ National Strategy for Combating Weapons of Mass Destruction (2006)
- 1087 ▪ National Strategy for Counterterrorism (2011)
- 1088 ▪ Quadrennial Homeland Security Review (QHSR) Report (2010)
- 1089 ▪ Preventive Radiological/Nuclear Detection (PRND) Capability Development Framework
- 1090 ▪ PRND National Incident Management System Resource Typing
- 1091 ▪ HSPD-7: Critical Infrastructure Identification, Prioritization, and Protection
- 1092 ▪ HSPD-9: Defense of Food and Agriculture
- 1093 ▪ HSPD-10: Biological Weapons Defense
- 1094 ▪ HSPD-13/NSPD-41: Maritime Security
- 1095 ▪ HSPD-19: Combating Terrorist Use of Explosives in the United States
- 1096 ▪ HSPD-22: Domestic Chemical Defense
- 1097 ▪ HSPD-21: National Biodefense Strategy and National Strategy for Countering Biological Threats
- 1098 ▪ United States Code Title 18: Illegal Use of WMD/CBRN

- 1099 ▪ Federal Terrorist Use of Explosives (TUE), August, 2008
- 1100 ▪ Federal Improvised Nuclear Device, Strategic Guidance Statement (SGS), September 2008
- 1101 ▪ Federal Improvised Nuclear Device, Strategic Plan, January 2009
- 1102 ▪ Federal Biological Attack (BIO), Strategic Guidance Statement, January 2009
- 1103 ▪ Federal Radiological Attack (RDD), Strategic Guidance Statement, January 2009
- 1104 ▪ Federal Chemical Attack (CML), Strategic Guidance Statement, June 2009
- 1105 ▪ Federal RDD Attack, Strategic Plan, July 2009
- 1106 ▪ Federal BIO Attack, Strategic Plan, July 2009
- 1107 ▪ DHS Suitability Program

1108 **Other.**

- 1109 ▪

1110

1111

DRAFT

1112 **Appendix 5 to Annex C: Defense of Agriculture and Food**

1113 **Key Authorities and References.**

1114 The following laws, policy directives, strategies, plans, and executive orders are included in addition
1115 to the general authorities/references provided in the base plan for the Defense of Agriculture and
1116 Food Mission Activity.

- 1117 ▪ Food and Agriculture Sector-Specific Plan (2010)
- 1118 ▪ Food and Agriculture Sector Annual Reports (2010 & 2011)
- 1119 ▪ National Infrastructure Protection Plan (2009)
- 1120 ▪ National Annual Reports (2010 & 2011)
- 1121 ▪ Strategic National Risk Assessment (2011)
- 1122 ▪ NSPD-17/HSPD-4: National Strategy to Combat Weapons of Mass Destruction
- 1123 ▪ HSPD-5: Management of Domestic Incidents
- 1124 ▪ HSPD-7: Critical Infrastructure Identification, Prioritization, and Protection
- 1125 ▪ HSPD- 9: Defense of United States Agriculture and Food
- 1126 ▪ HSPD-10: National Policy for Biodefense
- 1127 ▪ Presidential Policy Directive 2: National Strategy for Countering Biological Threats
- 1128 ▪ Food and Drug Administration (FDA) Food Safety Modernization Act of 2011
- 1129 ▪ Farm Security and Rural Investment Act of 2002, PL 107-171, Subtitle E, Animal Health
1130 Protection, Section 10401-10418
- 1131 ▪ Title 7 Code of Federal Regulations §371.5(b)(7)
- 1132 ▪ Section 1337 of the Agriculture and Food Act of 1981 (P.L. 97-98)
- 1133 ▪ Humane Methods of Slaughter Act (7 U.S.C. §§ 1901-1906)
- 1134 ▪ Federal Anti-Tampering Act (18 U.S.C. § 1365, 35 U.S.C. § 155A)
- 1135 ▪ National Strategy for Biosurveillance (in development)
- 1136 ▪ Title 10 U.S.C. 371 - 382.
- 1137 ▪ Title 18 U.S.C. 229E. Chapter 10, titled Biological Weapons
- 1138 ▪ Title 42 U.S.C. 3771
- 1139 ▪ Title 28 U.S.C. 533.
- 1140 ▪ 28 Code of Federal Regulations §0.85
- 1141 ▪ Homeland Security ACT of 2002 (6 U.S.C., Section 101 et seq.) Section 302
- 1142 ▪ Executive Order 13486: Working Group on Strengthening Laboratory Security in the United
1143 States
- 1144 ▪ Executive Order 13546: Optimizing the Security of Biological Select Agents and Toxins in the
1145 United States

- 1146 ▪ TITLE 42--Public Health, CHAPTER I--PUBLIC HEALTH SERVICE, DEPARTMENT OF
1147 HEALTH AND HUMAN SERVICES, SUBCHAPTER F--QUARANTINE, INSPECTION,
1148 LICENSING, PART 73--SELECT AGENTS AND TOXINS
- 1149 ▪ TITLE 7—Agriculture, Subtitle B--REGULATIONS OF THE DEPARTMENT OF
1150 AGRICULTURE, CHAPTER III--ANIMAL AND PLANT HEALTH INSPECTION SERVICE,
1151 DEPARTMENT OF AGRICULTURE, PART 331--POSSESSION, USE, AND TRANSFER OF
1152 SELECT AGENTS AND TOXINS
- 1153 ▪ Title 9--Animals and Animal Products, CHAPTER I--ANIMAL AND PLANT HEALTH
1154 INSPECTION SERVICE, DEPARTMENT OF AGRICULTURE, PART 121--POSSESSION,
1155 USE, AND TRANSFER OF SELECT AGENTS AND TOXINS
- 1156 ▪ Federal Import Milk Act (1927)
- 1157 ▪ Federal Food, Drug, and Cosmetic Act of 1938, as amended
- 1158 ▪ Public Health Service Act (1944)
- 1159 ▪ Fair Packaging and Labeling Act (1966)
- 1160 ▪ Infant Formula Act of 1980, as amended
- 1161 ▪ Nutrition Labeling and Education Act of 1990
- 1162 ▪ Dietary Supplement Health and Education Act of 1994
- 1163 ▪ Agricultural Marketing Act of 1946, Section 203(h), 7 U.S.C. 1621-1627 - Authorizes the
1164 Secretary of Agriculture to inspect, certify and identify the class, quality, quantity, and condition
1165 of agricultural products when shipped or received in interstate commerce.
- 1166 ▪ Agricultural Marketing Act of 1946, 7 U.S.C. 74 - Grain Inspection, Packers, and Stockyards
1167 Administration (GIPSA) administers and enforces certain inspection and standardization
1168 activities related to rice, pulses, lentils, and processed grain products such as flour and corn meal,
1169 as well as other agricultural commodities.
- 1170 ▪ Agricultural Marketing Act of 1946, Section 203(j), 7 U.S.C. 1621 - Authorizes the Secretary of
1171 Agriculture to assist in improving transportation services and facilities, and in obtaining equitable
1172 and reasonable transportation rates and services and adequate transportation facilities for
1173 agricultural products and farm supplies. Agricultural Marketing Service (AMS) may conduct,
1174 assist, and foster research, investigation, and experimentation to determine the best methods of
1175 transporting agricultural products; and foster and assist in the development of new or expanded
1176 markets (domestic and foreign) for moving larger quantities of agricultural products through the
1177 private marketing system to consumers in the United States and abroad.
- 1178 ▪ Agricultural Marketing Act of 1946, Section 203(k), 7 U.S.C. 1621 - Authorizes the Secretary of
1179 Agriculture to collect, tabulate, and disseminate statistics on marketing agricultural products,
1180 including, but not restricted to, statistics on market supplies, storage stocks, quantity, quality, and
1181 condition of such products in various positions in the marketing channel, utilization of such
1182 products, and shipments and unloads thereof.
- 1183 ▪ Agricultural Reform and Improvement Act of 1996, 7 U.S.C. 950aaa - Encourages and improves
1184 telemedicine and distance learning services in rural areas through the use of telecommunications,
1185 computer networks, and related advanced technologies by students, teachers, medical
1186 professionals, and rural residents.

- 1187 ▪ Agricultural Research Act of 1935, 7 U.S.C. 427 - Authorizes the Secretary of Agriculture to
1188 ensure agriculture a position in research equal to that of industry, which will aid in maintaining
1189 an equitable balance between agriculture and other sections of the economy.
- 1190 ▪ Agricultural Research and Marketing Act of 1946, 7 U.S.C. 1621-1627, 1624 specifically -
1191 Authorizes the Secretary of Agriculture to cooperate with other entities, including branches of
1192 Federal government, State agencies, and private research organizations in producing,
1193 transporting, storing, processing, marketing, and distributing agricultural products in any and all
1194 jurisdictions.
- 1195 ▪ Agriculture Marketing Act of 1946, 7 U.S.C. 1621-1627 - Congress resolved that the prosperity
1196 of the Nation depends on an efficient, private system for distributing and marketing agricultural
1197 products. To achieve this goal, the Agriculture Marketing Act of 1946 was passed to provide for
1198 continuous research to improve agriculture marketing, cooperation between Federal and State
1199 agencies, and to integrate the administration of laws enacted by Congress to aid the distribution
1200 of agricultural products.
- 1201 ▪ Animal Health Protection Act, 7 U.S.C. 8301 - Authorizes the Secretary of Agriculture to
1202 prohibit or restrict the importation, exportation, and interstate movement of animals or other
1203 articles as necessary to prevent pests or diseases of livestock (any farm-raised animals, including
1204 fish) from being introduced into, or disseminated within, the United States.
- 1205 ▪ Animal Welfare Act, 7 U.S.C. 2146 - Authorizes the Secretary of Agriculture to promulgate
1206 regulations and standards governing the humane handling, care, treatment, and transportation of
1207 animals, as defined in the act, by dealers, exhibitors, and other regulated persons.
- 1208 ▪ Child Nutrition Act of 1966, as amended - Authorizes child nutrition programs (National School
1209 Lunch Program, School Breakfast Program, Child and Adult Care Food Program, and Summer
1210 Food Service Program) and the Special Supplemental Nutrition Program for Women, Infants, and
1211 Children (WIC). The programs provide States with cash, commodity, and other assistance,
1212 including nutrition services and food packages in the WIC program. Food and Nutrition Service
1213 (FNS) administers these programs at the Federal level.
- 1214 ▪ Egg Products Inspection Act (EPIA), 21 U.S.C. 1031 et seq. - Food Safety and Inspection
1215 Service (FSIS) provides continuous inspection of all egg products prepared for distribution in
1216 commerce and re-inspects imported products to ensure they meet U.S. food safety standards.
1217 FSIS tests for and conducts enforcement activities to address microbiological, chemical, and
1218 other types of contamination and conducts epidemiological investigations in cooperation with
1219 Centers for Disease Control and Prevention (CDC) based on reports of food-borne health hazards
1220 and disease outbreaks.
- 1221 ▪ Farm Security and Rural Investment Act of 2002, Public Law 107-171, Title X, Subtitle E -
1222 Consolidates a number of pre-existing animal health-related statutes into a single comprehensive
1223 law; among other items, authorizes the Secretary of Agriculture to prohibit or restrict the
1224 importation, exportation, and interstate movement of animals or other articles as necessary to
1225 prevent pests or diseases of livestock from being introduced into, or disseminated within, the
1226 United States; and authorizes the Secretary to issue any regulations or orders considered
1227 necessary to carry out the Animal Health Protection Act. Also reauthorized the Emerson Trust
1228 through 2007. (See Bill Emerson Humanitarian Trust in this table).
- 1229 ▪ Federal Meat Inspection Act (FMIA), 21 U.S.C. 601 et seq. - FSIS provides continuous
1230 inspection of all meat products prepared for distribution in commerce and re-inspects imported
1231 products to ensure they meet U.S. food safety standards. FSIS tests for and conducts enforcement

- 1232 activities to address microbiological, chemical, and other types of contamination and conducts
1233 epidemiological investigations in cooperation with CDC based on reports of food-borne health
1234 hazards and disease outbreaks.
- 1235 ■ Food Quality Protection Act 1996, Public Law 104-170 - Authorizes the Pesticide Data Program
1236 to develop and communicate comprehensive, statistically reliable information on pesticide
1237 residues in food to improve government dietary risk assessment procedures.
- 1238 ■ Food, Agriculture, Conservation, and Trade Act of 1990, 7 U.S.C. 950aaa - Encourages and
1239 improves telemedicine services and distance learning services in rural areas through
1240 telecommunications, computer networks, and related technologies.
- 1241 ■ Launching Our Communities Access to Local Television Act of 2000, 47 U.S.C. 1101 -
1242 Facilitates access to signals of local television stations for households in non-served and
1243 underserved areas.
- 1244 ■ National Agricultural Research, Extension, and Teaching Policy Act of 1977, as amended, 7
1245 U.S.C. 3121-3122 - The enactment of subsequent laws modified, extended, or added new
1246 research authorities for Agricultural Research Service (ARS).
- 1247 ■ Organic Act of 1862, 7 U.S.C. 2201 - The act is the main authority for the establishment of the
1248 USDA and ARS.
- 1249 ■ Packers and Stockyards Act of 1921, 7 U.S.C. 181 - Prohibits unfair, deceptive, and fraudulent
1250 practices by market agencies, dealers, packers, swine contractors, and live poultry dealers in the
1251 livestock, poultry, and meatpacking industries.
- 1252 ■ Plant Protection Act (PPA) (Title IV of the Agricultural Risk Protection Act of 2000, Public Law
1253 106-224) - Consolidates pre-existing pest quarantine and exclusion statutes into a single
1254 comprehensive law; authorizes the Secretary of Agriculture to prohibit or restrict the importation,
1255 exportation, and interstate movement of plants, plant products, biological control organisms,
1256 noxious weeds, plant pests, or other articles as necessary to prevent plant pests or noxious weeds
1257 from being introduced into, or disseminated within, the United States; authorizes the Secretary to
1258 issue any regulations or orders that the Secretary considers necessary to carry out the PPA.
- 1259 ■ Poultry Products Inspection Act (PPIA), 21 U.S.C. 451 et seq. - FSIS provides continuous
1260 inspection of all poultry products prepared for distribution in commerce and re-inspects imported
1261 products to ensure that they meet U.S. food safety standards. FSIS tests for and conducts
1262 enforcement activities to address microbiological, chemical, and other types of contamination
1263 and conducts epidemiological investigations in cooperation with CDC based on reports of food-
1264 borne health hazards and disease outbreaks.
- 1265 ■ Public Health Security and Bioterrorism Preparedness and Response Act of 2002, Public Law
1266 107-188 - To improve the ability of the United States to prevent, prepared for, and respond to
1267 bioterrorism and other public emergencies.
- 1268 ■ U.S. Grain Standards Act of 1916, 7 U.S.C. 79 - Congress established the Federal grain
1269 inspection entity in 1976 to manage the national grain inspection system and institute a national
1270 grain-weighing program.
- 1271 ■ Virus-Serum-Toxin Act of 1913, 21 U.S.C. 151-159 - Authorizes the Secretary of Agriculture to
1272 regulate veterinary biologics (vaccines, bacterins, antisera, diagnostic kits, and other products of
1273 biological origin) to ensure that the veterinary biologics available for the diagnosis, prevention,
1274 and treatment of animal diseases are pure, safe, potent, and effective.

- 1275 ▪ Wholesome Meat Act 1967, 21 U.S.C. 601 - FSIS is responsible for assessing whether State
1276 inspection programs that regulate meat are at least equal to the Federal program. The act
1277 extended FSIS jurisdiction over meat and meat products granting authority to regulate
1278 transporters, renderers, cold storage warehouses, and animal-food manufacturers.

1279 **Other.**

- 1280 ▪
- 1281
- 1282

DRAFT

1283 **Appendix 6 to Annex C: Health Security**

1284 **Key Authorities and References.**

1285 The following laws, policy directives, strategies, plans, and executive orders are included in addition
1286 to the general authorities/references provided in the base plan for the Health Security Mission
1287 Activity:

- 1288 ▪ The Pandemic and All-Hazards Preparedness Act (PAHPA) , 2006
- 1289 ▪ National Health Security Strategy (NHSS), presented to Congress in December 2009 and to be
1290 subsequently revised every four years afterward.
- 1291 ▪ Section 2802 of the Public Health Service Act.
- 1292 ▪ Food, Drug and Cosmetic Act.
- 1293 ▪ Health Insurance Portability and Accountability Act (HIPAA).
- 1294 ▪ Health Information Technology for Economic and Clinical Health (HITECH) Act.

1295 **Other.**

- 1296 ▪

1297

1298

DRAFT

1299 **Appendix 7 to Annex C: Immigration Security**

1300 **Key Authorities and References.**

1301 The following laws, policy directives, strategies, plans, and executive orders are included in addition
1302 to the general authorities/references provided in the base plan for the Immigration Security Mission
1303 Activity.

- 1304 ▪ National Southwest Border Counternarcotics Strategy (June 2009)
- 1305 ▪ The National Security Strategy, May 2010.
- 1306 ▪ The Partnership for 21st Century U.S. Southwest Border Security, April 2010.
- 1307 ▪ The Quadrennial Homeland Security Review (QHSR), February 2010.
- 1308 ▪ The Quadrennial Defense Review (QDR), February 2010.

1309 **Other.**

- 1310 ▪

1311

1312

DRAFT

1313 **Appendix 8 to Annex C: Maritime Security**

1314 **Key Authorities and References.**

1315 The following laws, policy directives, strategies, plans, and executive orders are included in addition
1316 to the general authorities/references provided in the base plan for the Maritime Security Mission
1317 Activity.

- 1318 ▪ National Southwest Border Counternarcotics Strategy (June 2009)
- 1319 ▪ The National Security Strategy, May 2010.
- 1320 ▪ The Partnership for 21st Century U.S. Southwest Border Security, April 2010.
- 1321 ▪ The 2010 National Drug Control Strategy.
- 1322 ▪ The National Southwest Border Counternarcotics Strategy, June 2009.
- 1323 ▪ The Quadrennial Homeland Security Review (QHSR), February 2010.
- 1324 ▪ The Quadrennial Defense Review (QDR), February 2010.
- 1325 ▪ The National Interdiction Command and Control Plan (NICCP), March 2010.
- 1326 ▪ DHS Maritime Migration Plan (DMMP), April 2011
- 1327 ▪ DHS Operations Plan – VIGILANT SENTRY (OVS), August, 200.
- 1328 ▪ The Department of Justice Strategy for Combating Mexican Cartels, November 2009.
- 1329 ▪ The Maritime Operations Coordination Plan (MOC-P)
- 1330 ▪ National Strategy for Maritime Security (September 2005)
- 1331 ▪ Maritime Operational Threat Response for the National Strategy for Maritime Security (October
1332 2006)
- 1333 ▪ National Strategy for the Marine Transportation System: A Framework for Action (July 2008)
- 1334 ▪ National Strategy for Physical Protection of Critical Infrastructure and Key Assets (February
1335 2003)
- 1336 ▪ National Strategy for Global Supply Chain Security
- 1337 ▪ National Plan to Achieve Maritime Domain Awareness (October 2005)
- 1338 ▪ National Infrastructure Protection Plan (NIPP)
- 1339 ▪ Maritime Transportation System Security Plan
- 1340 ▪ Maritime Transportation Security Act of 2002
- 1341 ▪ DHS Small Vessel Security Strategy, April 2008
- 1342 ▪ DHS Small Vessel Security Strategy Implementation Plan, January 2011
- 1343 ▪ The U.S. Coast Guard Strategy for Maritime Safety, Security, and Stewardship (January 19,
1344 2007)
- 1345 ▪ Area Maritime Security Plans
- 1346 ▪ Maritime Infrastructure Recovery Plan (2006)

- 1347 ▪ Maritime Operational Threat Response Plan (2006)
- 1348 ▪ Outer Continental Shelf Facility Security Plans
- 1349 ▪ Plans to Re-establish Cargo Flow after TSI, 2005 SSI only
- 1350 ▪ Underwater Terrorism Preparedness Plans
- 1351 ▪ United States Coast Guard Combating Maritime Terrorism Strategic and Performance Plan
1352 (2008)
- 1353 ▪ Vessel and Facility Security Plans
- 1354 ▪ Transportation Systems Sector-Specific Plan (TS SSP)
- 1355 ▪ National Maritime Transportation Security Plan (NMTSP), Annex B: Maritime
- 1356
- 1357
- 1358

DRAFT

1359 **Appendix 9 to Annex C: Protection of Key Leadership and**
1360 **Events**

1361 **Key Authorities and References.**

1362 The following laws, policy directives, strategies, plans, and executive orders are included in addition
1363 to the general authorities/references provided in the base plan for the Key Leadership and Special
1364 Events Security Mission Activity.

- 1365 ▪ Title 18 USC Sections 3056 and 3056A (amended 2005)
- 1366 ▪ Title 18 USC Section 2332b (f)
- 1367 ▪ Executive Order 12333 Intelligence and Counterintelligence
- 1368 ▪ Executive Order 12656 National Security Emergency Preparedness
- 1369 ▪ NSPD-46 (2007)
- 1370 ▪ NSPD-47
- 1371 ▪ Homeland Security Act (2002)
- 1372 ▪ HSPD 5
- 1373 ▪ HSPD 7 (2003)
- 1374 ▪ HSPD 15 (2007)
- 1375 ▪ HSPD-16
- 1376 ▪ HSPD-19
- 1377 ▪ National Response Framework
- 1378 ▪ Memorandum of the AG on Coordination of Explosives Investigations and Related Matters,
1379 August 11, 2004
- 1380 ▪ DHS Information Sharing Strategy (April 2008)
- 1381 ▪ Memorandum of the DHS Secretary on the establishment of the Special Events Program in DHS
1382 Office of Operations Coordination and Planning (OPS) (October 2007)

1383

1384

1385 **Appendix 10 to Annex C: Transportation Security**

1386 **Key Authorities and References.**

1387 The following laws, policy directives, strategies, plans, and executive orders are included in addition
1388 to the general authorities/references provided in the base plan for the Transportation Security Mission
1389 Activity.

1390 **Statutes and Regulations**

- 1391 ▪ 49 U.S.C. §§ 101 and 301.
- 1392 ▪ The Aviation and Transportation Security Act, 49 U.S.C. § 40101 note (2007), as amended.
- 1393 ▪ The Homeland Security Act of 2002, codified predominately at 6 U.S.C. §§ 101-557 (2002), as
1394 amended.
- 1395 ▪ The Post-Katrina Emergency Management Reform Act of 2006, title VI of the Department of
1396 Homeland Security Appropriates Act, 2007, Pub. L. 109-295.
- 1397 ▪ The Economy Act, 31 U.S.C. § 1535 et seq. (2007).
- 1398 ▪ Public Health Service Act, 42 U.S.C. § 264 (2011), as amended
- 1399 ▪ The Robert T. Stafford Disaster Relief and Emergency Assistance Act, 42 U.S.C. § 5121 et seq.
1400 (2007), as amended.
- 1401 ▪ The Maritime Transportation Security Act, codified predominately at 46 U.S.C. §§ 70102-70117
1402 (2007).
- 1403 ▪ Intelligence Reform and Terrorism Prevention Act of 2004, 50 U.S.C 401 note, (2004), as
1404 amended.
- 1405 ▪ The National Emergencies Act, 50 U.S.C. § 1601 et seq. (2007).
- 1406 ▪ Defense Production Act of 1950, 50 U.S.C. App. § 2061 et seq. (2009), as amended.
- 1407 ▪ The Defense Against Weapons of Mass Destruction Act, 50 U.S.C. § 2301 et seq. (2007).

1408 **Executive Orders**

- 1409 ▪ Executive Order 12148, Federal Emergency Management, July 20, 1979, as amended.
- 1410 ▪ Executive Order 12656, Assignment of Emergency Preparedness Responsibilities, November 18,
1411 1988, as amended.
- 1412 ▪ Executive Order 12657, Federal Emergency Management Agency Assistance in Emergency
1413 Preparedness Planning at Commercial Nuclear Power Plants, November 18, 1988, as amended.
- 1414 ▪ Executive Order 12742, National Security Industrial Responsiveness, January 8, 1991, as
1415 amended.
- 1416 ▪ Executive Order 13286, Amendment of Executive Orders, and Other Actions, in Connection with
1417 the Transfer of Certain Functions to the Secretary of Homeland Security, March 5, 2003, as
1418 amended.
- 1419 ▪ Executive Order 13434, National Security Professional Development, May 17, 2007.
- 1420 ▪ Executive Order 13603, National Defense Resources Preparedness, March 16, 2012.

1421 ***Presidential Decision Directives, National Security Presidential Directives and Homeland Security***
1422 ***Presidential Directives***

- 1423 ▪ Presidential Decision Directive-39 (PDD-39): U.S. Policy on Counter-terrorism, June 21, 1995.
- 1424 ▪ Presidential Decision Directive-62 (PDD-62): Protection Against Unconventional Threats to the
1425 Homeland and Americans Overseas, May 22, 1998.
- 1426 ▪ Presidential Decision Directive-63 (PDD-63): Critical Infrastructure Protection, May 22, 1998.
- 1427 ▪ Homeland Security Presidential Directive 1 (HSPD-1): Organization and Operation of the
1428 Homeland Security Council, October 29, 2001.
- 1429 ▪ Homeland Security Presidential Directive 5 (HSPD-5): Management of Domestic Incidents,
1430 February 28, 2003.
- 1431 ▪ Homeland Security Presidential Directive 7 (HSPD-7): Critical Infrastructure Identification,
1432 Prioritization, and Protection, December 17, 2003.
- 1433 ▪ Homeland Security Presidential Directive 13/National Security Presidential Directive 41:
1434 Maritime Security Policy, December 21, 2004.
- 1435 ▪ Homeland Security Presidential Directive 16: National Strategy for Aviation Security, March 6,
1436 2006.
- 1437 ▪ Homeland Security Presidential Directive 19: Combating Terrorist Use of Explosives in the
1438 United States, March 29, 2007.
- 1439 ▪ Homeland Security Presidential Directive 21: Public Health and Emergency Preparedness,
1440 October 18, 2007.
- 1441 ▪ Homeland Security Presidential Directive 23/National Security Presidential Directive 54: Cyber
1442 Security and Monitoring, January 8, 2008.
- 1443 ▪ National Security Presidential Directive 44 (NSPD 44) Management of Interagency Efforts
1444 concerning Reconstruction and Stabilization, December 7, 2005.
- 1445 ▪ National Security Presidential Directive 51 (NSPD 51)/Homeland Security Presidential Directive
1446 20 (HSPD 20), National Continuity Policy, May 9, 2007.
- 1447 ▪ Presidential Policy Directive 1: Organization of National Security Council System, February 13,
1448 2009.
- 1449 ▪ Presidential Policy Directive 2: Implementation of National Strategy for Countering Biological
1450 Threats, November 23, 2009.
- 1451 ▪ Presidential Policy Directive 8: National Preparedness, March 30, 2011.

1452 ***Other***

- 1453 ▪ National Incident Management System, March 1, 2004.
- 1454 ▪ National Strategy for Pandemic Influenza Implementation Plan, December 2006.
- 1455 ▪ National Continuity Policy Implementation Plan, August 2007.
- 1456 ▪ National Response Framework, January 2008.
- 1457 ▪ Federal Continuity Directive 1 and Federal Continuity Directive 2, February 2008.

1458

1459

DRAFT

1460 **Annex D: Selected Glossary/Lexicon**

- 1461 **Capability Targets:** The performance threshold(s) for each core capability.
- 1462 **Core Capabilities:** Distinct critical elements necessary to achieve the National Preparedness Goal.
- 1463 **Critical Infrastructure:** Systems and assets, whether physical or virtual, so vital to the United States
1464 that the incapacity or destruction of such systems and assets would have a debilitating impact on
1465 security, national economic security, national public health or safety, or any combination thereof.
1466 The Nation’s critical infrastructure is composed of 18 sectors.
- 1467 **Critical Tasks:** Lorem Ipsum
- 1468 **Cybersecurity:** Encompasses the cyberspace global domain of operations consisting of the
1469 interdependent network of information technology infrastructures, and includes the Internet,
1470 telecommunications networks, computer systems, and embedded processors and controllers in
1471 critical industries. The cybersecurity core capability is the means for protecting cyberspace from
1472 damage, unauthorized use, or exploitation of electronic information and communications systems and
1473 the information contained therein to ensure confidentiality, integrity, and availability.
- 1474 **Imminent Threat:** Intelligence or operational information that warns of a credible, specific, and
1475 impending terrorist threat or ongoing attack against the United States and its territories that is
1476 sufficiently specific and credible to recommend implementation of protective measures to thwart or
1477 mitigate against an attack.
- 1478 **Enhanced Steady State:** Lorem Ipsum
- 1479 **Mission Areas:** Groups of core capabilities, including Prevention, Protection, Mitigation, Response,
1480 and Recovery.
- 1481 **Mitigation:** The capabilities necessary to reduce loss of life and property by lessening the impact of
1482 disasters.
- 1483 **National Health Security:** The Nation and its people are prepared for, protected from, and resilient
1484 in the face of health threats or hazards with potentially negative health consequences.
- 1485 **National Preparedness:** The actions taken to plan, organize, equip, train, and exercise to build and
1486 sustain the capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and
1487 recover from those threats that pose the greatest risk to the security of the Nation.
- 1488 **Performance Measure:** The metrics used to ascertain actual performance against target levels
1489 identified for each core capability; by design, they are clear, objective, and quantifiable.
- 1490 **Prevention:** The capabilities necessary to avoid, prevent, or stop a threatened or actual act of
1491 terrorism. For the purposes of the prevention framework called for in PPD-8, the term “prevention”
1492 refers to preventing imminent threats.
- 1493 **Protection:** The capabilities necessary to secure the homeland against acts of terrorism and
1494 manmade or natural disasters.
- 1495 **Recovery:** The capabilities necessary to assist communities affected by an incident to recover
1496 effectively.
- 1497 **Resilience:** The ability to adapt to changing conditions and withstand and rapidly recover from
1498 disruption due to emergencies.

1499 **Response:** The capabilities necessary to save lives, protect property and the environment, and meet
1500 basic human needs after an incident has occurred.

1501 **Risk Assessment:** A product or process that collects information and assigns a value to risks for the
1502 purpose of informing priorities, developing or comparing courses of action, and informing decision
1503 making.

1504 **Security:** The protection of the Nation and its people, vital interests, and way of life.

1505 **Stabilization:** The process by which the immediate impacts of an incident on community systems are
1506 managed and contained.

1507 **Steady State:** Lorem Ipsum

1508 **Terrorism:** Any activity that involves an act that is dangerous to human life or potentially
1509 destructive of critical infrastructure or key resources and is a violation of the criminal laws of the
1510 United States or of any state or other subdivision of the United States; and, appears to be intended to
1511 intimidate or coerce a civilian population, or to influence the policy of a government by intimidation
1512 or coercion, or to affect the conduct of a government by mass destruction, assassination, or
1513 kidnapping. (Note that although the definition of terrorism includes both domestic and international
1514 acts of terrorism, the scope of the planning system is the prevention and protection against acts of
1515 terrorism in the homeland.)

1516 **Weapon of Mass Destruction:** Any destructive device; any weapon that is designed or intended to
1517 cause death or serious bodily injury through the release, dissemination, or impact of toxic or
1518 poisonous chemicals or their precursors; any weapon involving a biological agent, toxin, or vector; or
1519 any weapon that is designed to release radiation or radioactivity at a level dangerous to human life.

1520 **Whole Community:** A focus on enabling the participation in national preparedness activities of a
1521 wider range of players from the private and nonprofit sectors, including nongovernmental
1522 organizations and the general public, in conjunction with the participation of Federal, state, and local
1523 governmental partners in order to foster better coordination and working relationships. Used
1524 interchangeably with “all-of-Nation.”