Critical Infrastructure Protection and Federal Statutory Authority for the Departments of Homeland Security and Defense to Perform Two Key Tasks

A Monograph

by

Ms. Patricia Ladnier
US Department of Homeland Security

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas

2017

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
13-04-2017	Master's Thesis	June 2016-May 2017

4. TITLE AND SUBTITLE
Critical Infrastructure Protection and Federal Statutory Authority for the Departments of Homeland Security and Defense to Perform Two Key Tasks

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Patricia Ladnier

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
Fort Leavenworth, KS 66027-2301

8. PERFORMING ORG REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
School of Advanced Military Studies
Advanced Military Studies Program
Fort Leavenworth, KS 66027

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The fields of study are national security, critical infrastructure protection, homeland security and defense, government, public policy, and law. The research question is whether the Departments of Homeland Security (DHS) and Defense (DOD) have federal statutory authority to perform two tasks key to protect critical infrastructure: establish standards and physically protect and secure infrastructure when an owner fails to do so. Such authority is lacking. The federal government has constitutional authority for national security. The federal government identified critical infrastructure protection as vital, to be achieved through public-private partnership. This survey of federal statutes relevant to physical critical infrastructure reveals a lack of strategic, integrated authority to implement needed measures when others fail to act. The DHS has assessed homeland security and promoted public-private partnership for years. To ensure that critical infrastructure is protected, the DHS needs further statutory authority. The DHS and the DOD need certainty about working together, especially in a crisis. The federal statutory framework needs to be commensurate with constitutional authority and responsibility for national security so as to lessen gaps between lofty goals mandated for these departments and reasonable actionable authority to accomplish their missions.

15. SUBJECT TERMS
Critical infrastructure protection; federal statutory authority (or law); Department of Homeland Security; Department of Defense; establish standards; physical protection and security; national security

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
					Patricia Ladnier
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. PHONE NUMBER** *(include area code)*
(U)	(U)	(U)	(U)	63	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

Monograph Approval Page

Name of Candidate:	Ms. Patricia Ladnier
Monograph Title:	Critical Infrastructure Protection and Federal Statutory Authority for the Departments of Homeland Security and Defense to Perform Two Key Tasks

Approved by:

_____, Monograph Director
Melissa A. Thomas, PhD

_____, Seminar Leader
Marc A. Spinuzzi, COL

_____, Director, School of Advanced Military Studies
James C. Markert, COL

Accepted this 25th day of May 2017 by:

_____, Director, Graduate Degree Programs
Prisco R. Hernandez, PhD

Abstract

Critical Infrastructure Protection and Federal Statutory Authority for the Departments of Homeland Security and Defense to Perform Two Key Tasks, by Ms. Patricia Ladnier, 63 pages.

The fields of study are national security, critical infrastructure protection, homeland security and defense, government, public policy, and law. The research question is whether the Departments of Homeland Security (DHS) and Defense (DOD) have federal statutory authority to perform two tasks key to protect critical infrastructure: establish standards and physically protect and secure infrastructure when an owner fails to do so. Such authority is lacking.

The federal government has constitutional authority for national security. The federal government identified critical infrastructure protection as vital, to be achieved through public-private partnership. This survey of federal statutes relevant to physical critical infrastructure reveals a lack of strategic, integrated authority to implement needed measures when others fail to act. The DHS has assessed homeland security and promoted public-private partnership for years. To ensure that critical infrastructure is protected, the DHS needs further statutory authority. The DHS and the DOD need certainty about working together, especially in a crisis. The federal statutory framework needs to be commensurate with constitutional authority and responsibility for national security so as to lessen gaps between lofty goals mandated for these departments and reasonable actionable authority to accomplish their missions.

Contents

Acronyms

ADP	Army Doctrine Publication
ADRP	Army Doctrine Reference Publication
CFATS	Chemical Facilities Anti-Terrorist Standards
CIPA	Critical Infrastructures Protection Act of 2001
CRS	US Congressional Research Service
DHS	US Department of Homeland Security
DOD	US Department of Defense
DOJ	US Department of Justice
DOT	US Department of Transportation
FEMA	Federal Emergency Management Agency, DHS
FPS	Federal Protective Service, NPPD, DHS
GAO	US General Accountability Office
GSA	US General Services Administration
JP	Joint Publication
NPPD	National Protection and Programs Directorate, DHS
NRF	National Response Framework
OIP	Office of Infrastructure Protection, NPPD, DHS
PPD-21	Presidential Policy Directive 21
US	United States
US Code	*United States Code*
USCG	US Coast Guard

Illustrations

Tables

Section One: Introduction

Both the Department of Homeland Security (DHS) and the Department of Defense (DOD) work to secure and defend the United States, including protecting and securing key resources and critical infrastructure (referred to in this monograph collectively as "critical infrastructure"). The Constitution and federal statutory law establish national security goals. The Critical Infrastructures Protection Act of 2001 (CIPA) articulates as a national security goal the protection of critical infrastructure by a public-private partnership.[1] The Homeland Security Act of 2002 specifically tasks the DHS with preventing terrorism and protecting critical infrastructure.[2] Much of the nation's critical infrastructure is interdependent and interconnected and is not owned by the federal government.[3] Critical infrastructure sustained damage in multiple post-9/11 disasters or emergencies. Reports about some of these catastrophes analyze lessons learned. Two key tasks for critical infrastructure protection emerge as crucial: (1) establishing standards and enforcing compliance with the standards; and (2) physically protecting and securing critical infrastructure routinely and in an emergency. Reviewing relevant existing federal statutory authority for the DHS and the DOD to perform these two key tasks reveals that authority for the DHS and the DOD is insufficient to achieve these two protective tasks. A strategic review

[1] Critical Infrastructures Protection Act of 2001, Public Law 107-56, title X, §1016, *Statutes at Large* 115 (2001): 400, codified at *US Code* 42 (2017), §5195c, accessed March 21, 2017, http://uscode.house.gov/browse.xhtml. All references to the *US Code* in this monograph were accessed from this website as of March 21-25, 2017; any statutory changes since March 21-25, 2017 are not reflected in this survey of federal statutory law.

[2] Homeland Security Act of 2002, Public Law 107-296, *US Statutes at Large* 116 (2002): 2135, codified at *US Code* 6 (2017), §§101 *et seq*.

[3] ICF International, *Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats* (June 2016), 88, 91, accessed March 22, 2017, https://energy.gov/epsa/downloads/electric-grid-security-and-resilience-establishing-baseline-adversarial-threats; James K. Hayes and Charles K. Ebinger, “The Private Sector and the Role of Risk and Responsibility in Securing the Nation's Infrastructure,” *Journal of Homeland Security and Emergency Management* 18, no. 1 (March 2011): 2, accessed April 2, 2017, https://www.brookings.edu/wp-content/uploads/2016/06/04_critical_infrastructure_ebinger.pdf.

should realign federal statutory law to allow the DHS to implement recommendations to achieve its national security goal of critical infrastructure protection.

Section two explains the constitutional authority for US national security and how it has been implemented historically by the DOD and now by both the DHS and the DOD. The statutory framework to implement constitutional authority historically authorized the DOD to defend the nation and to support national defense policies. The CIPA linked national security and critical infrastructure protection. “Critical infrastructure” is an asset or a system that, if incapacitated or destroyed, "would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[4] After 9/11, the Homeland Security Act of 2002 created and authorized the DHS for the mission of homeland security to prevent terrorism, reduce vulnerability to terrorism, and prepare for and respond to terrorism and other disasters and emergencies. The DHS entities most concerned with critical infrastructure protection are the National Protection and Program Division's (NPPD) Federal Protective Service (FPS) and Office of Infrastructure Protection (OIP), the Federal Emergency Management Agency (FEMA), and the US Coast Guard (USCG). This background frames the critical infrastructure protection policy and responsibilities.

Section three discusses the CIPA's framing of critical infrastructure protection as a public-private partnership where infrastructure owners and government share responsibility. CIPA and Presidential Policy Directive-21 (PPD-21) designated specific infrastructures or "sectors" as critical. PPD-21 states that infrastructure owners are best suited to manage risks and to determine security strategies. PPD-21 assigned specific federal entities as responsible sector specific agencies. The DHS is responsible for eight of the sixteen sectors and for another two in conjunction with the General Services Administration (GSA) and the Department of

[4] *US Code* 42 (2017), §5195c(e).

Transportation (DOT). The CIPA and PPD-21 explicitly state as national policy reliance on a public-private partnership for critical infrastructure protection. Recent events, including physical attacks on the electric grid and the 2010 British Petroleum Deepwater Horizon oil well failure disaster, cast doubt on this reliance. This doubt is compounded when considering that non-federal infrastructure sectors, including foreign owners, own much of US critical infrastructure. Multiple reports from some post-9/11 disasters and emergencies provide observations, conclusions, and recommendations about critical infrastructure protection. One key task for critical infrastructure protection discussed in these reports is to establish standards and enforce compliance. A second key task is to physically protect and secure the critical infrastructure routinely and in an emergency. These reports made many recommendations for protective measures. These two key tasks are used in this paper because they appeared in multiple reports and illustrate basic protective measures. These two key tasks are the basis for evaluating the existing federal statutory authority for the DHS and the DOD to protect critical infrastructure.

Section four explores whether DHS entities most relevant to critical infrastructure protection have federal statutory authority to perform these two key tasks, including where the owner fails to adequately protect the infrastructure. The CIPA and Homeland Security Act contain no new regulatory authority for critical infrastructure protection. The DHS has limited statutory authority to establish standards and enforce compliance and to physically protect and secure critical infrastructure. Finally, this section discusses some challenges the DHS faces in exercising its existing federal statutory authority, with a conclusion that the DHS has limited authority to achieve critical infrastructure protection.

Section five examines federal statutory authority for the DOD to achieve the two key tasks. No statutory authority exists for the DOD to issue regulations to set standards for critical infrastructure protection, which is appropriate for our civilian government. As for the second key task, the DOD's statutory authority would encompass physically protecting and securing critical

infrastructure but only in certain emergency-type situations. Further, multiple challenges experienced by the DOD in executing its existing federal statutory authority could exacerbate or compromise the DOD's ability to protect critical infrastructure in a crisis.

Three conclusions reached from examining federal statutory authority in sections four and five are set forth in section six. First, the DHS regulatory authority to set standards is very limited and offers no mechanism for an integrated, strategic regulatory framework for critical infrastructure protection. Second, the DHS and the DOD statutory authority to physically protect and secure critical infrastructure routinely and in an emergency is limited to specific sectors and circumstances. Third, no statute defines how the DHS and the DOD are to work together to achieve national security and, more specifically, critical infrastructure protection, even in an emergency or a crisis. The Homeland Security Act makes clear that the DHS mission is separate from the DOD mission and reaffirms the DOD statutory authority. However, it offers no authority for an integrated response or single command authority.[5] These conclusions show a deficiency in the current federal statutory authority.

A strategic review of national security policy should examine policy assumptions and practicalities of critical infrastructure protection. Such a review should result, where warranted, in strategic, integrated policy revisions and realign statutory authority with mission accomplishment. The policy and assumptions in CIPA, PPD-21, and the Homeland Security Act rely upon the public-private partnership paradigm to achieve critical infrastructure protection. Also, regulatory

[5] *US Code* 6 (2017), §456. William C. Banks and Stephen Dycus, *Soldiers on the Home Front: The Domestic Role of the American Military* (Cambridge, MA: Harvard University Press, 2016), 11. US Congressional Research Service (CRS), *Defining Homeland Security: Analysis and Congressional Considerations*, by Shawn Reese, R42462 (Washington, DC, January 8, 2013), Summary, accessed April 2, 2017, https://fas.org/sgp/crs/homesec/R42462.pdf. This CRS report concludes that the US government does not have a single definition for "homeland security" which may impede the development of a coherent national homeland security strategy and "may hamper the effectiveness of Congressional oversight."

authority that may cover critical infrastructure is diffused among multiple separate DHS entities and federal agencies that historically have been concerned with safety issues, not national security. Almost sixteen years have passed since 9/11 and the CIPA. Multiple reports warn of gaps in critical infrastructure protection.[6] Two other specific considerations identified in this review could be addressed with statutory amendments: repealing the statute that criminalizes *posse comitatus* and fixing the dual command problem. Section six ends with a caution that, in a crisis, people likely want and will demand immediate, easy-to-understand, easy-to-see government action. That is why it is important to be proactive in strategically reviewing national security and critical infrastructure protection policy and the statutory framework that authorizes critical infrastructure protection.

[6] US General Accountability Office (GAO), *Critical Infrastructure Protection: DHS Has Made Progress in Enhancing Critical Infrastructure Assessments, but Additional Improvements are Needed, Testimony before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Committee on Homeland Security, House of Representatives*, by Chris Currie, GAO-15-692T (Washington, DC, July 12, 2016), accessed April 2, 2017, http://docs.house.gov/meetings/HM/HM08/20160712/105169/HH"RG-114-HM08-Wstate-CurrieC-20160712.pdf; US CRS, *Blackout! Are We Prepared to Manage the Aftermath of a Cyber-Attack or Other Failure of the Electrical Grid?* Written Testimony Before US Congress, by Richard Campbell (Washington, DC: US Government Printing Office, April 2016), quoted in Blackout! Are We Prepared to Manage the Aftermath of a Cyber-Attack or Other Failure of the Electrical Grid? Hearing before the Committee on Transportation and Infrastructure, 114th Cong., 2d sess., April 14, 2016, 65, accessed January 16, 2017, https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg99931/pdf/CHRG-114hhrg99931.pdf; California Public Utilities Commission, *Regulation of Physical Security for the Electric Distribution System*, by Ben Brinkman, Connie Chen, Arthur O'Donnell, and Chris Parkes (February 2015), 3, 6, 13, accessed March 22, 2017, https://pdfs.semanticscholar.org/e11b/21010c0fa8e68d0958496bc3564c50524c63.pdf; Center for the Study of the Presidency and Congress (CSPC), *Securing the U.S. Electrical Grid: Understanding the Threats to the Most Critical of Critical Infrastructure, While Securing a Changing Grid*, by Thomas F. McLarty III and Thomas J. Ridge (Washington, DC: CSPC, October 2014), accessed January 5, 2017, https://www.thepresidency.org/sites/default/files/Final%20Grid%20Report_0.pdf.

The DHS has made much progress toward a safer, more resilient nation as detailed in reports to Congress by the DHS and the General Accountability Office (GAO).[7] Now it needs the tools to move to the next level to ensure implementation of recommendations from assessments and studies.[8] This paper is a survey of the federal statutory authority most relevant to protecting the nation's critical infrastructure generally and as a whole. The scope is focused in two respects. First, the DHS entities studied are the ones concerned generally with working to protect all sectors of critical infrastructure: NPPD's FPS and OIP; FEMA; and the USCG. This paper does not consider highly technical and specialized sectors, such as cyber, nuclear, and nuclear waste, or a DHS entity that is responsible for one specific function, such as the Transportation Security Administration. Second, the plain text of federal statutes is reviewed, without reference to

[7] US DHS, NPPD, *Written Testimony of NPPD Office of Infrastructure Protection Assistant Secretary Caitlin Durkovich and NPPD Office of Cybersecurity and Communications Assistant Secretary Andy Ozment for a House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies Hearing Titled "Value of DHS" Vulnerability Assessments in Protecting Our Nation's Critical Infrastructure* (Washington, DC, July 12, 2016), accessed April 2, 2017, https://www.dhs.gov/news/2016/07/12/written-testimony-nppd-house-homeland-security-subcommittee-cybersecurity; US GAO, *Critical Infrastructure Protection: DHS Has Made Progress in Enhancing Critical Infrastructure Assessments*; US DHS, *The 2014 Quadrennial Homeland Security Review* (Washington, DC, June 18, 2014), accessed April 2, 2017, www.dhs.gov/sites/default/files/publications/qhsr/2014-QHSR.pdf.

[8] Some thought-provoking articles relevant to issues in homeland security and defense that question the effectiveness of our current status include: Steven Brill, “Is America Any Safer? 15 Years after 9/11," *The Atlantic*, September 2016, accessed April 4, 2017, http://www.theatlantic.com/magazine/archive/2016/09/are-we-any-safer/492761/. Brill argues that much progress has been made in homeland security, but gaps remain. Barry Friedman, “We Spend $100 Billion on Policing. We have No Idea What Works. Police Are More Likely to Adopt New Technology Because Another Department Has It Than Because of Reasoned Cost-Benefit Analysis,” *The Washington Post*, March 10, 2017, accessed March 12, 2017, https://www.washingtonpost.com/posteverything/wp/2017/03/10/we-spend-100-billion-on-policing-we-have-no-idea-what-works/?hpid=hp_no-name_opinion-card-b%3Ahomepage%2Fstory&utm_term=.e3f11d7fbd8c. Friedman discusses the increasing cost of policing, including weapons and other systems, and questions effectiveness of expensive new technology. Douglas Heaven, “The Uncertain Future of Democracy,” *BBC*, March 30, 2017, accessed March 30, 2017, http://www.bbc.com/future/story/20170330-the-uncertain-future-of-democracy. Heaven discusses trends in democratic countries, including alarming moves in some countries toward the certainty and security offered by authoritarianism.

interpretation through federal executive agency regulations or judicial case law. Reviewing more than the plain meaning of the statutes exceeds the scope of this monograph. Also, this approach serves as a test of whether the plain meaning is understandable to the general public, as well as public servants trying to administer laws, rather than focusing on understandability by lawyers or people who can access lawyers and legal research.

The challenge of critical infrastructure protection is highly relevant now – not only because of terrorism but also because of infrastructure aging and decay and the looming need to invest heavily in it. These circumstances present an opportunity to adopt standards to compel compliance with the standards, through regulation if needed, and also to ensure clear authority for physical protection and security where an owner fails to adequately protect the infrastructure. Given the interdependent and networked nature of the nation's critical infrastructure, it is important to build on years of work by the DHS. The DHS has worked to assess the critical infrastructure and build partnerships and frameworks for public-private collaboration. The next logical step is to shepherd the nation through implementing recommendations from assessments and collaborative efforts to ensure that the critical infrastructure is protected and the nation is resilient in a crisis.

Section Two: National Security and Critical Infrastructure Protection

An understanding of the constitutional and statutory framework for national security and critical infrastructure protection is necessary before beginning the analysis of the DHS and the DOD federal statutory authority for protecting the nation's critical infrastructure. The US Constitution's preamble highlights security as part of the purpose for establishing the Constitution: "to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defence, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity." The Constitution grants to the federal government authority and responsibility for national security. Early federal statutes enabled the military to protect the nation. More recent statutory law authorizes the DHS to protect the homeland from terrorism. Recent national policy recognizes the priority of protecting critical infrastructure as vital to the nation's security and relies on a public-private partnership solution.[9]

DOD and DHS Missions for Homeland Defense and Homeland Security

Individual military services historically have implemented the constitutional mandates to protect the United States, culminating in consolidating the Army, Navy and Marine Corps, and Air Force into the DOD after World War II.[10] Statutes define these services' functions as follows:

---

[9] US Constitution, preamble; art. 1, sec. 8; art. 4, sec. 4. The Constitution states that the federal government is: "[to] provide for the common Defence and general Welfare of the United States;" "to provide for calling forth the Militia to execute the Laws of the Union, suppress Insurrections and repel Invasions"; "to [guarantee] every State … a Republican Form of Government, and [to] protect … against Invasion; and … against domestic Violence" [upon request of the state]. Banks and Dycus, 43-46; Stephen I. Vladeck, "Emergency Power and the Militia Acts," *Yale Law Journal* 114 (2004): 149-194, accessed February 20, 2017, http://www.yalelawjournal.org/pdf/427_pa9skxwv.pdf. These sources provide a history of federal statutes authorizing the use of military force on the home front, enacted shortly after ratification of the Constitution and continuing to more modern times. Thomson Reuters, *Guide to Homeland Security* (Eagan, MN: Thomson Reuters, 2016), 1-5. This source gives background on the DHS.

[10] The National Security Act of 1947, Public Law 114-328, chapter 343, §2, *US Statutes at Large* 61 (1947): 496, codified at *US Code* 50 (2017), §3002.

Table 1. Statutory Purpose for Army, Air Force, Navy, and Marine Corps

Army	Air Force
"(1) preserving the peace and security, and providing for the defense, of the United States, …; (2) supporting the national policies; (3) implementing the national objectives; and (4) overcoming any nations responsible for aggressive acts that imperil the peace and security of the United States." *USC Code* 10 (2017), §3062(a).	"(1) preserving the peace and security, and providing for the defense, of the United States, …; (2) supporting the national policies; (3) implementing the national objectives; and (4) overcoming any nations responsible for aggressive acts that imperil the peace and security of the United States." *USC Code* 10 (2017), §8062(a).
Navy	**Marine Corps**
"for prompt and sustained combat incident to operations at sea. It is responsible for the preparation of naval forces necessary for the effective prosecution of war except as otherwise assigned." *US Code* 10 (2017), §5062.	"to provide fleet marine forces of combined arms, together with supporting air components, for service with the fleet in the seizure or defense of advanced naval bases and for the conduct of such land operations as may be essential to the prosecution of a naval campaign. In addition, the Marine Corps … shall provide security detachments for the protection of naval property at naval stations and bases, and shall perform other duties as the President may direct." *US Code* 10 (2017), §5063.

Source: Author, created from identified sections of the *US Code* (2017), Title 10 (Armed Forces).

The DOD is responsible for protecting the nation through homeland defense[11] and supporting national policies. DOD doctrine defines homeland defense as "the protection of US sovereignty, territory, domestic population, and critical infrastructure against external threats and aggression, or other threats as directed by the President."[12]

[11] US DOD, Joint Chiefs of Staff, *Joint Publication 3-27, Homeland Defense* (Washington, DC, July 29, 2013), accessed March 23, 2017, http://www.dtic.mil/doctrine/new_pubs/jp3_27.pdf; US DOD, Joint Chiefs of Staff, *Joint Publication 3-28, Defense Support of Civil Authorities* (Washington, DC, July 31, 2013), accessed March 23, 2017, http://dtic.mil/doctrine/new_pubs/jp3_28.pdf; US DOD, Department of the Army, Headquarters, *Army Doctrine Publication (ADP) 3-28, Defense Support of Civil Authorities* (Washington, DC, July 2012), accessed March 23, 2017, http://www.apd.army.mil/epubs/DR_pubs/DR_a/pdf/web/adp3_28.pdf; US DOD, Department of the Army, Headquarters, *Army Doctrine Reference Publication (ADRP) 3-28, Defense Support of Civil Authorities* (Washington, DC, June 2013), accessed March 23, 2017, http://www.apd.army.mil/epubs/DR_pubs/DR_a/pdf/web/adrp3_28.pdf.

[12] US DOD, *Joint Publication 3-27, Homeland Defense*, I-1.

The more recent Homeland Security Act of 2002 created the DHS. The DHS entities most directly responsible for physical critical infrastructure protection of multiple infrastructure sectors are the NPPD, FEMA, and USCG.[13] NPPD includes the FPS, which protects federal government property,[14] and the OIP, created by the Act to promote protection of critical infrastructure generally. The FEMA previously was an independent federal agency focused on disaster and emergency preparedness and response and now also works toward infrastructure protection and resilience. The USCG is a military service and a branch of the armed forces, transferred from the DOT. It may operate as part of the US Navy upon a Congressional declaration of war or when the president directs.[15] The USCG's mission is to protect and defend US ports, inland waterways, coastline, and territorial waters (referred to collectively as US ports, waters, and coastline). This chart summarizes the major relevant responsibilities of the DHS and these DHS entities:

[13] US DHS, "Organizational Chart," DHS, last modified February 1, 2017, 1 and 21, accessed March 25, 2017, https://www.dhs.gov/organizational-chart. Portions of the DHS organization chart depicting the organizational placement within the DHS of these entities are in Appendix 1. *US Code* 6 (2017), §121 (NPPD), §311 *et seq*. (FEMA); Coast Guard and Maritime Transportation Act of 2012, Public Law 112-213, *US Statutes at Large* 126 (2012): 1540, codified at *US Code*, Title 14 (Coast Guard); *US Code* 14, §3.

[14] It exceeds the scope of this monograph to parse overlaps in protective functions among FPS and other commonly known specific government personnel and buildings, such as, for example, the White House protected by the US Secret Service and the US Capitol protected by the US Capitol Police. For this analysis, it is sufficient to focus on FPS as the responsible entity for protecting government property in general.

[15] *US Code* 14 (2017), §1, §3(a) and (b).

Table 2. DHS and DHS Entities with Critical Infrastructure Protection Missions

<table>
<tr><th>DHS</th><th>NPPD</th></tr>
<tr><td rowspan="3">"The primary mission of the Department is to
(A) prevent terrorist attacks within the United States;
(B) reduce the vulnerability of the United States to terrorism;
(C) minimize the damage, and assist in the recovery, from terrorist attacks that do occur within the United States;
(D) carry out all functions of entities transferred to the Department, including by acting as a focal point regarding natural and manmade crises and emergency planning; …." US Code 6 (2017), §111(b).</td><td>FPS (and designated DHS employees)</td></tr>
<tr><td>"shall protect the buildings, grounds, and property that are owned, occupied or secured by the Federal Government … and the persons on the property." US Code 40 (2017), §1315(a).</td></tr>
<tr><td>OIP
"(1) To access, receive, and analyze law enforcement information, intelligence information, and other information …. to –
(A) identify and assess the nature and scope of terrorist threats to the homeland;
(B) detect and identify threats of terrorism against the United States; ….
(2) To carry out comprehensive assessments of the vulnerabilities of key resources and critical infrastructure ….
(3) To integrate relevant information, analysis, and vulnerability assessments … to –
(A) identify priorities for protective and support measures regarding terrorist and other threats to homeland security ….
(5) To develop a comprehensive national plan for securing the key resources and critical infrastructure of the United States…." US Code 6 (2017), §121(d).</td></tr>
<tr><th>FEMA</th><th>Coast Guard</th></tr>
<tr><td>"… to reduce the loss of life and property and protect the Nation from all hazards, including natural disasters, acts of terrorism, and other man-made disasters by leading and supporting the Nation in a risk-based, comprehensive emergency management system of preparedness, protection, response, recovery, and mitigation.
…. lead the Nation's efforts to prepare for, protect against, respond to, recover from, and mitigate against the risk of natural disasters, acts of terrorism, and other man-made disasters, including catastrophic incidents; …. providing the Federal Government's response to terrorist attacks and major disasters, including (A) managing such response; … (D) coordinating other Federal response resources…. US Code 6 (2017), §313(b)(1), (2)(A); §314(a)(3).</td><td>"(1) enforce or assist in the enforcement of all applicable Federal laws on, under, and over the high seas and waters subject to the jurisdiction of the United States;
(2) engage in maritime air surveillance or interdiction to enforce or assist in the enforcement of the laws of the United States;
(3) administer laws and promulgate and enforce regulations for the promotion of safety of life and property on and under the high seas and waters subject to [US] jurisdiction,….
(7) maintain … readiness to function as a specialized service in the Navy in time of war, …. US Code 14 (2017), §2.</td></tr>
</table>

Source: Author, created from identified sections of the *US Code* (2017), Title 6 (Domestic Security) and Title 14 (Coast Guard).

The DHS has broad and specific statutory authority for homeland security[16] and critical infrastructure protection. Both the DOD and DHS have missions for securing the homeland and its critical infrastructure and for supporting national policies.

National Security Policy to Protect Critical Infrastructure

National security policy identifies critical infrastructure protection as vital, as articulated in the CIPA:

> A continuous national effort is required to ensure the reliable provision of cyber and physical infrastructure services critical to maintaining the national defense, continuity of government, economic prosperity, and quality of life ….
>
> It is the policy of the United States – (1) that any physical or virtual disruption of the operation of the critical infrastructures of the United States be rare, brief, geographically limited in effect, manageable, and minimally detrimental to the economy, human and government services, and national security of the United States; and that actions necessary to achieve the policy stated in paragraph (1) be carried out in a public-private partnership involving corporate and non-governmental organizations….[17]

The CIPA defined critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[18] The CIPA relies upon "a public-private partnership" for acting to protect critical infrastructure.

---

[16] *US Code* 6 (2017), §101. The Homeland Security Act defines “American homeland” and “homeland” as “the United States” but contains no definition for homeland security. US DHS, “Our Mission,” last modified May 11, 2016, accessed April 4, 2017, https://www.dhs.gov/our-mission. The DHS states: “The vision of homeland security is to ensure a homeland that is safe, secure, and resilient against terrorism and other hazards.” Christopher Bellavita, “Changing Homeland Security: What is Homeland Security?” *Homeland Security Affairs* 4 (June 2008), accessed April 4, 2017, https://www.hsaj.org/articles/118.

[17] *US Code* 42 (2017), §5195c(b)(3) and (c)(1), (2).

[18] *US Code* 42 (2017), §5195c(e).

Conclusion

The Constitution empowers the federal government to secure the nation. Historically, this role fell to the DOD. In 2002, the DHS received the mission of homeland security. National policy, expressed through the CIPA, established critical infrastructure protection as a national security priority. The public-private paradigm for achieving critical infrastructure protection and lessons learned about critical infrastructure protection from some post-9/11 disasters and emergencies are explored in section three.

Section Three: The Public-Private Sectors as Partners to Protect Critical Infrastructure

The CIPA's framing of critical infrastructure protection as a shared action of infrastructure owners and government may not result in protected critical infrastructure. This "sharing" assumes reaching consensus on protection measures and implementation. Studies of some disaster and emergency scenarios cast doubt on this assumption. The ownership of US critical infrastructure magnifies this doubt since private entities, non-federal public entities (such as state and local governments or utilities), and non-federal public-private entities own much of it. These studies demonstrate this tension and make recommendations to improve critical infrastructure protection. Two key tasks for protecting critical infrastructure emerge from these recommendations: establishing standards and physically protecting and securing the infrastructure.

The Public-Private Sectors Partnership

The CIPA assumes that the private and public sectors would reach consensus and act in partnership. PPD-21 takes this assumption a step further by stating: "Critical infrastructure owners and operators are uniquely positioned to manage risks to their individual operations and assets, and to determine effective strategies to make them more secure and resilient."[19] The CIPA highlighted certain infrastructure sectors and functional areas as critical. PPD-21 subsequently defined sixteen critical infrastructure sectors and assigned responsible sector specific agencies to each. This chart summarizes these CIPA and PPD-21 designations:

[19] Barack Obama, Presidential Policy Directive 21, "Directive on Critical Infrastructure Security and Resilience" (February 12, 2013), Introduction, accessed March 21, 2017, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil; https://www.hsdl.org/?view&did=731087.

Table 3. Critical Infrastructure Designations in the CIPA and PPD-21

CIPA		**PPD-21**
Function	**Sector**	**Sector with Designated Sector Specific Agency**
	Telecommunications	Chemical: DHS
	Energy	Commercial facilities: DHS
	Financial services	Communications: DHS
	Water	Critical manufacturing: DHS
	Transportation	Dams: DHS
National defense		Defense industrial base: DOD
Government continuity		Emergency services: DHS
Economic prosperity		Energy: Energy
Quality of life		Financial services: Treasury
		Food-agriculture: Agriculture, Health & Human Services
		Government facilities: DHS, GSA
		Healthcare-public health: Health & Human Services
		Information Technology: DHS
		Nuclear: DHS
		Transportation: DHS, DOT
		Water, wastewater: Environmental Protection Agency

Source: Author, created from information in the CIPA and PPD-21.

Recent physical attacks on the electric grid and the 2010 Deepwater Horizon oil well failure and oil spill, among other examples, cast doubt on the assumption underlying the CIPA and PPD-21.[20] This doubt is important since non-federal entities own much of critical infrastructure and since some of it is foreign owned.[21] As an example, buildings owned by foreign

[20] ICF International, 88, 91. This report was prepared for the US and the Canadian governments. It demonstrates that the majority of utilities are investor owned and that it is difficult to achieve results across the grid. California Public Utilities Commission, 3, 6, 13. The 2011 and 2013 electric grid exercises revealed private owners had not implemented available security measures. National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, *Deepwater: The Gulf Oil Disaster and the Future of Offshore Drilling, Report to the President* (Washington, DC: US Government Printing Office, January 11, 2011), 118-127, accessed April 2, 2017, https://www.gpo.gov/fdsys/pkg/GPO-OILCOMMISSION/content-detail.html. Problems with design and protective measures and with management practices and oversight by owner and subcontractors caused the disaster.

[21] Hayes and Ebinger; Strategic Foresight Initiative, *Critical Infrastructure: Long-term Trends and Drivers and Their Implications for Emergency Management* (June 2011), accessed April 2, 2017, https://www.fema.gov/pdf/about/programs/oppa/critical_infrastructure_paper.pdf. This research and report was prepared for the FEMA. US Department of State, Under Secretary for Democracy and Global Affairs, "Critical Infrastructure Protection," Department of State Archive. August 2007, accessed April 2, 2007, https://2001-2009.state.gov/g/avianflu/91243.htm. This article discusses how critical infrastructure is interconnected even outside of the United States, including in Canada and Mexico. Christopher Bellavita, "85% of What You Know about Homeland Security is Probably

entities, including from non-NATO countries such as China, house some highly secure government agencies. A recent GAO report concluded that these leasing arrangements pose security risks for this infrastructure sector.[22] Two key facts call into question whether critical infrastructure protection is satisfactory: (1) continued critical infrastructure vulnerabilities and (2) privately owned infrastructure being outside of the government's control. [23] Reports of recent critical infrastructure damage demonstrate how to measure the ability of the federal government to ensure that critical infrastructure truly is protected.

Wrong," *Homeland Security Watch*, March 16, 2009, accessed April 2, 2017, http://www.hlswatch.com/2009/03/16/85-percent-is-wrong/. This author critiques the commonly used eighty-five percent figure used to describe private sector ownership of critical infrastructure. US CRS, *Blackout!* Campbell gives an example from the electric grid where only nine federal electric utilities are federally owned; 189 are investor owned; 2,013 are publicly owned by non-federal entities; and 887 are consumer owned.

[22] US GAO, *Federal Real Property: GSA Should Inform Tenant Agencies When Leasing High-Security Space from Foreign Owners*, by David Wise, GAO-17-195 (Washington, DC, January 2017), 2, 13, 20, accessed April 2, 2017, http://www.gao.gov/products/GAO-17-195; Sophie Tatum and Pamela Brown, "First on CNN: Report Finds National Security Agencies at Risk in Foreign-Owned Buildings," *CNN*, January 30, 2017, accessed February 1, 2017, http://www.cnn.com/2017/01/30/politics/gao-report-foreign-ownership/; US CRS, *The Committee on Foreign Investment in the United States (CFIUS)*, by James K. Jackson, RL33388 (Washington, DC, February 19, 2016), 30-31, accessed April 2, 2017, https://www.hsdl.org/?view&did=790777.

[23] US CRS, *Issues in Homeland Security Policy for the 113th Congress*, by William L. Painter, R42985 (Washington, DC, February 27, 2013), 3, accessed April 2, 2017, https://www.hsdl.org/?view&did=732600. In addition, the report crystallizes a key point. Arguably, "homeland security, at its core, is about coordination because of the disparate stakeholders and risks …. Without a general consensus on the literal and philosophical definition of homeland security, … some believe that there will continue to be the potential for disjointed and disparate approaches to securing the nation."

Lessons from Some Post-9/11 Disasters and Emergencies

Some specific post-9/11 disaster and emergencies illustrate threats and damage to critical infrastructure regardless of whether the crisis is from natural or human causes or whether unintentional or intentional. Reports about the Northwest US-Canadian electric grid failure (2003), Hurricane Katrina (2005), Deepwater Horizon oil well failure and oil spill (2010), and physical attacks on the Metcalf, California electric substation (2013-14) recommend critical infrastructure protection measures and provide examples of protection shortfalls and gaps.

Key Task: Standards—Establishing Standards and Enforcing Compliance

Multiple reports studying specific emergencies recommend that the government establish specific standards and enforce compliance. The 2003 US-Canada task force recommended that US and Canadian government agencies establish and enforce compliance with reliability standards "in the planning, design, and operation of North America's vast bulk power systems."[24] More recent reports continue to echo the need for greater electric grid regulation. [25] The Deepwater Horizon commission specifically concluded that a lack of government standards contributed to the disaster.[26] The question then becomes how to set standards. The 2008 EMP commission report succinctly stated the allocation of responsibility between industry and government and why the government must set standards:

---

[24] US-Canada Power System Outage Task Force, *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations* (April 2004), 139, accessed January 16, 2017, https://energy.gov/oe/downloads/blackout-2003-final-report-august-14-2003-blackout-united-states-and-canada-causes-and.

[25] ICF International, 88, 91; California Public Utilities Commission; US GAO, *Critical Infrastructure Protection: DHS Has Made Progress in Enhancing Critical Infrastructure Assessments*, 6-7, 10, 16-17; National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, 118-127.

[26] National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, 118-127.

> Industry is responsible for assuring system reliability, efficiency, and cost effectiveness as a matter of meeting required service levels to be paid for by its customers. Government is responsible for protecting the society and its infrastructure, including the electric power system. Only government can deal with barriers to attack — interdiction before consequence. Only government can set the standards necessary to provide the appropriate level of protection against catastrophic damage from EMP for the civilian sector.[27]

Two main points are the allocation of responsibility between industry and government and the independence of government from industry.

The government's independence from the infrastructure owner is crucial. Both the US-Canada and the Deepwater Horizon commissions criticized the government for relying too much on industry, to the detriment of both the public and workers at infrastructure facilities. The Deepwater Horizon Commission candidly stated that the government regulatory agency "had a built-in financial incentive [from charging expensive licensing and permitting fees] to promote offshore drilling that was in tension with its mandate to ensure safe drilling and environmental protection." Having the government set standards and enforce compliance gives infrastructure owners a common, independent guide for security concerns.[28]

---

[27] Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures* (April 2008), 53, accessed January 29, 2017, http://www.empcommission.org/docs/A2473-EMP_Commission-7MB.pdf.

[28] US-Canada Power System Outage Task Force, 21. National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, 126-127, 250-251. The National Commission stated that it is important to assure the “independence and integrity of government institutions charged with protecting the public interest.” The government agency did not adopt pending regulations, opposed by industry, “that would have required companies to manage all of their activities and facilities, and those of their contractors, under a documented Safety and Environmental Management System (SEMS)” until after this disaster. Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, 53-54, 57, 59-60, 80-81, 104, 155, 157, 173. As another example, the EMP Commission suggested standards that the DHS either would set itself or work with other government agencies to set. Suggested standards include: to require gasoline and diesel fuel distribution facilities to have on-site power generation in the event of electrical grid failure, for testing and installing electrical equipment, to require incorporation of new technology in telecommunications infrastructure, and to improve hardening of oil and gas control systems to avoid damage from EMP effects.

Key Task: Security—Physically Protecting and Securing Critical Infrastructure

The electric grid attacks and Katrina establish the need for routine physical security. The US electric power grid, historically concerned with deterring vandalism, now is "most vulnerable to intentional damage from malicious acts" to shut down an infrastructure or perpetrate a terrorist act. Despite voluntary guidelines, grid owners failed or declined to implement available security measures even at critical high voltage substations, as evidenced by substation attacks in California, Arkansas, and Arizona and results from North American Electric Reliability Corporation grid exercises in 2011 and 2013. A Congressional Research Service (CRS) report noted continuing efforts of the Federal Energy Regulatory Commission to implement its physical security policy for the power grid and recommended that Congress examine "whether company-specific security initiatives appropriately reflect the risk profiles of their particular assets, and whether additional security measures across the grid uniformly reflect terrorism risk from a national perspective."[29] On-going routine physical security of critical infrastructure is required.

Katrina and the collapse of law and order illustrate the need for emergency protection of critical infrastructure. The total collapse of local law enforcement led to uncontrolled violence and civil unrest. Katrina destroyed local government capabilities and incapacitated and overwhelmed state government, leading to calls for assistance from higher jurisdictional levels. The federal government experienced difficulty in protecting and restoring critical infrastructures

[29] US CRS, *Physical Security of the US Power Grid: High-Voltage Transformer Substations*, by Paul W. Parfomak, R43604 (Washington, DC, July 2, 2015), 2, 30, 32, accessed February 1, 2017, https://www.everycrsreport.com/files/20150702_R43604_df43c1c3c34ecca8d6730fcca7cff108bddd4a66.pdf; California Public Utilities Commission, iii-iv, 3, 6, 13, 29; ICF International, 14-16, 88, 91.

after Katrina. Eventually, federal forces were decisive in helping the state National Guard to restore order in New Orleans.[30]

Conclusion

National policy envisions critical infrastructure protection as achievable by public-private partnership. Recent events cast doubt on this assumption and highlight two key tasks that are crucial to protection: standard-setting and physical security. If the infrastructure owner fails to accomplish these two key tasks, the question becomes whether the DHS and the DOD has federal statutory authority to set standards for critical infrastructure protection and to physically protect and secure the infrastructure. The DHS and the DOD federal statutory authorities related to these two key tasks is the subject of sections four and five, respectively.

[30] Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina, A Failure of Initiative: Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina, 109th Cong., 2d sess., 2006, HR Rep. 109-377, 1, 3, accessed January 15, 2017, https://www.gpo.gov/fdsys/pkg/CRPT-109hrpt377/pdf/CRPT-109hrpt377.pdf; The White House, *The Federal Response to Hurricane Katrina: Lessons Learned*, by Frances Fragos Townsend (Washington, DC, February 23, 2006), 40-43, 61 accessed January 15, 2017, https://www.hsdl.org/?view&did=460536.

Section Four: Existing Federal Statutory Authority for the DHS

The DHS's NPPD, FEMA, and USCG have limited federal statutory authority to establish standards and to physically protect and secure critical infrastructure when the owner fails to adequately do so. The DHS has some regulatory authority for standard-setting for federal government property, areas under the jurisdiction of the USCG, and certain parts of the chemical sector. The only statutory authority to physically protect and secure critical infrastructure covers federal government property and certain USCG authorities. The DHS has challenges in effectively exercising its authorities to perform the identified two key tasks, including a lack of regulatory authority to effect an integrated response to protect critical infrastructure, especially where an owner fails to protect critical infrastructure.

Key Task: Standards—Establishing Standards and Enforcing Compliance

The CIPA and Homeland Security Act contain no new regulatory authority for critical infrastructure protection. The Homeland Security Act provides that the DHS has existing regulatory authority under three specified statutes and from authority previously granted to agencies transferred to the DHS. [31] Current regulatory authority for the DHS to establish standards and enforce compliance only addresses property owned or occupied by the federal

[31] *US Code* 6 (2017), §457, mandates that "[e]xcept as otherwise provided in sections 186(c) and 441(c) of [title 6] and section 1315 of title 40, this chapter vests no new regulatory authority [in the DHS] … and transfers … only such regulatory authority as exists on November 25, 2002, within any agency, program, or function transferred to the [DHS]… or that … is exercised by another official of the executive branch with respect to such agency, program, or function." The provisions of 6 *US Code* §186(c) and §441(c) are not relevant to this monograph, with §186(c) permitting the DHS to designate anti-terrorism technology for liability protection and §441(c) relating to research and development issues. Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014, Public Law 113-254, *US Statutes at Large* 128 (2014): 2898, codified at *US Code* 6 (2017), §621 et seq. and Consolidated Appropriations Act, 2008, Subtitle J, Secure Handling of Ammonium Nitrate, Public Law 110-161 (Title V, Section 563), *US Statutes at Large* 121 (2007): 2083, codified at *US Code* 6 (2017), §488 et seq. These laws amended the Homeland Security Act of 2002 and authorized new regulatory authority for these two specific programs directed only at the chemical sector.

government and persons on the property; US ports, waters, and coastline; and certain parts of the chemical sector.

Federal Government Property and Persons on the Property

The DHS has regulatory authority that would extend to setting and enforcing standards over facilities owned or occupied by the federal government and persons on such property. The plain language of 40 *US Code* §1315(b) directs prescribing "regulations necessary for the protection and administration of property owned or occupied by the Federal Government and persons on the property." The statutory text specifies "occupied" which includes property owned by any private and non-federal entity. The statute penalizes regulation violations with a fine, imprisonment, or both.

US Ports, Waters, and Coastline

US ports, waters, and the coastline are the jurisdiction of the USCG. The USCG has the regulatory authority to establish standards and enforce compliance both for security and for safety. The authority to regulate for safety provides additional authority to the extent that safety issues also compromise security.

First, the USCG can implement statutes related to port and maritime transportation security and to transportation and commercial shipping.[32] Second, statutory authority exists for regulation of vessels in US territorial waters when either the president declares a national

[32] Coast Guard Authorization Act of 2010, Public Law 111-281, title VIII, §820(a), *US Statutes at Large* 124 (2010): 3001, codified at *US Code* 46 (2017), §70124 (port security). This section authorizes that “the Secretary may issue regulations necessary to implement this chapter” [chapter 701 of Subtitle VII which includes port, vessel, and maritime transportation security issues]. *US Code* 14 (2017), §100. This section authorizes the USCG to enforce 46 *US Code* chapter 551, coastwise trade laws. For an overview, *see* USCG, "Authorities,” USCG, [no date or last modified date listed on website], accessed March 23, 2017, http://www.overview.uscg.mil/Authorities/.

emergency or the US Attorney General determines that an actual or anticipated mass migration of aliens en route to the United States requires an immediate federal response.[33]

Further, the USCG may regulate to promote safety of life and property using two statutes. It seems reasonable that safety would encompass security since security affects safety of life and property. The first safety statute directs that the USCG "shall … promulgate and enforce regulations for the promotion of safety of life and property on and under the high seas and waters subject to the jurisdiction of the United States, covering all matters not specifically delegated by law to some other executive department."[34] The second safety statute grants the USCG regulatory authority over vessels, including vessel "design, construction, alteration, repair and operation" and "the use of vessel stores and other supplies of a dangerous nature."[35] Finally, the USCG has regulatory authority for hazardous materials in commerce which also authorizes regulations related to transportation and pipelines.[36]

---

[33] *US Code* 50 (2017), §191. The statute specifies regulation by the Secretary of Transportation with presidential approval, but as explained in 6 *US Code* §457, this authority would be exercised by the DHS, with presidential approval, since the USCG was transferred from the DOT to the DHS. The statutory history and citations to the *US Statutes at Large* and public laws are set forth in the note to 50 *US Code* §191, beginning with the statute's origination and continuing with the two most recent amendments, The Omnibus Consolidated Appropriations Act, 1997, Public Law 104-208, div. C, title VI, §649, *US Statutes at Large* 110 (1996): 3009-711 and Coast Guard and Maritime Transportation Act of 2004, Public Law 108-293, title II, §223 *US Statutes at Large* 118 (2004): 1040.

[34] *US Code* 14 (2017), §2(3). Another provision tasks the USCG to "enforce or assist in the enforcement of all applicable Federal laws on, under, and over the high seas and waters subject to [US] jurisdiction." *US Code* 14 (2017), §2(1) (emphasis added). If the Federal Aviation Administration (FAA) or the US Air Force (USAF) do not regulate low-flying drones over US territorial waters, then this security gap would be ripe to assign to the USCG, unless it fits in the regulatory scheme of the FAA or USAF.

[35] Coast Guard Authorization Act of 2010, Public Law 111-281, title VI, §612, *US Statutes at Large* 124 (2010): 2970, codified at *US Code* 46 (2017), §1, §3306.

[36] USCG, "Authorities."

Chemical Sector

Two laws amending the Homeland Security Act authorize the DHS to establish standards and to enforce compliance related to parts of the chemical sector. First, the Chemical Facilities Anti-Terrorist Standards (CFATS) Program regulates any facility that holds any specified chemical in a quantity at or above the minimum quantity for the chemical specified in the regulation. The statute directs the Secretary to "establish risk-based performance standards designed to address high levels of security risk at covered chemical facilities." The statute permits enforcement by civil enforcement and by emergency order in certain circumstances.[37]

Second, the Secure Handling of Ammonium Nitrate statute grants regulatory authority for the "sale and transfer of ammonium nitrate" to "prevent the misappropriation or use of ammonium nitrate in an act of terrorism."[38] The statute focuses on registration and recording of transactions involving ammonium nitrate and does not mention physical security of facilities.

Key Task: Security—Physically Protecting and Securing Critical Infrastructure

The only sectors for which the Act authorizes the DHS to physically protect and secure critical infrastructure are (1) federal government property and persons on such property and (2) US ports, waters, and coastline. Neither the authority granted to the OIP nor to the FEMA include physically protecting and securing critical infrastructure if the owner fails to adequately do so.

---

[37] *US Code* 6 (2017), §621 *et seq*., §622(a)(2)(C) risk-based performance standards; §624, civil enforcement; §624(c), emergency orders; §627, promulgation of regulations to implement the CFATS law.

[38] *US Code* 6 (2017), §488a(a). The proposed regulation for the Secure Handling of Ammonium Nitrate would establish the Ammonium Nitrate Security Program. A regulation has not been issued to implement the statute. US DHS, “Ammonium Nitrate Security Program,” DHS. October 7, 2016, accessed March 23, 2017, https://www.dhs.gov/ammonium-nitrate-security-program.

Federal Government Property and Persons on the Property

Statutory law mandates that the DHS "shall protect the buildings, grounds, and property that are owned, occupied, or secured by the Federal Government (including any agency, instrumentality, or wholly owned or mixed-ownership corporation thereof) and the persons on the property." The statute specifies that the DHS may designate employees of the DHS, including FPS personnel, for this purpose.[39]

US Ports, Waters, and Coastline

The statutory authority for the USCG does not mention specifically the physical protection of critical infrastructure so the analysis must rely upon reasonable inferences. First, the USCG has broad statutory authority to assist "any Federal agency, State, Territory, possession, or political subdivision thereof, or the District of Columbia, to perform any activity for which such personnel and facilities are especially qualified."[40] This statute requires a request for assistance from the proper authority as a precondition to action. This broad authority would include physically protecting and securing critical infrastructure either routinely or in an emergency since the USCG has training and equipment for defense.

In addition, the USCG has broad authority to routinely enforce laws related to US ports, waters, and coastline, including maritime shipping and transportation. The USCG enforces laws, conducts maritime air surveillance, and makes "inquiries, examinations, inspections, searches, seizures, and arrests upon the high seas and waters over which the United States has jurisdiction, for the prevention, detection, and suppression of violations of" US laws."[41] This authority enables

---

[39] Homeland Security Act of 2002, Public Law 107-296, title XVII, §1706(b)(1), *US Statutes at Large* 116 (2002): 2317, codified at *US Code* 40 (2017), §1315(b)(1).

[40] *US Code* 14 (2017), §141.

[41] *US Code* 14 (2017), §2(1), (2), law enforcement, maritime aerial surveillance; §89, law enforcement; §95(a)(1), (2) and §99, carrying firearms and making arrests; *US Code* 14 (2017), §100, authority to enforce chapter 551 of title 46, coastwise trade laws (shipping and

the USCG, as part of its routine mission, to protect critical infrastructure to the extent laws prohibit behavior affecting security (as opposed, for example, to collecting revenue or policing for safety hazards).

At certain specific times, statutory authority empowers USCG action that could include protecting and securing critical infrastructure. The USCG protects waterways and enforces regulations for anchorage and movement of vessels when the president declares a national emergency or when the US Attorney General "determines that an actual or anticipated mass migration of aliens en route to, or arriving off the coast of, the United States" requires an immediate federal response.[42] Finally, the USCG is a military service that maintains readiness for war and that operates as part of the US Navy when designated.[43] These authorities, while not specifically delineating critical infrastructure protection, enable the USCG to protect and secure critical infrastructure related to maritime transportation and related commercial facilities and shipping and other critical infrastructure when requested by the proper authority.

Challenges for the DHS in Exercising This Statutory Authority

Federal Government Property and Persons on the Property

In comparing two provisions of 40 *US Code* §1315, the statutory text differs. This difference could affect the regulatory scope since what is defined as subject to protection is greater than what is defined as subject to regulation:

transportation); *US Code* 14 (2017), §143. USCG officers “are deemed to be officers of the customs … subject to regulations issued by the Secretary of the Treasury governing officers of the customs”. For additional information, *see* USCG, “Authorities.”

[42] *US Code* 50 (2017), §191.

[43] *US Code* 14 (2017), §2(7), §1, and §3.

Table 4. Comparison of 40 *US Code* §1315(a) and (c)

Protection authority	Regulatory authority
mandates protection of "the **buildings, grounds**, and property that are owned, occupied, or **secured**" by the federal government and "persons on the property." *US Code* 40 (2017), §1315(a).	"may prescribe regulations necessary for the protection and administration of property owned or occupied" by the federal government and "persons on the property…" *US Code* 40 (2017), §1315(c).

Source: Author created. Emphasis added by underlining and by highlighting in bold the text in (a) that is not in (c); the difference represents a gap in defined authority to protect and to regulate.

US Ports, Waters, and Coastline

The USCG's broad statutory authority to regulate for defense and law enforcement and to protect US ports, waters, and coastline does not explicitly specify protecting critical infrastructure when an owner fails to adequately do so. Also, some of its authority can be exercised only in times of emergency or war or upon specific request. Finally, the broad authority in 6 *US Code* §141 is unclear as to whether it is limited to areas traditionally in the USCG jurisdiction (high seas; US ports, waters, and coastline) or is broader.

The USCG, as a military service, faces the confusion surrounding the doctrine of *posse comitatus* and laws limiting its use. For centuries, this doctrine permitted local sheriffs to assemble help in enforcing the law and restoring order. "*Posse comitatus*" is Latin for "power of the county" or "the force of the county." The practice dates to English law as early as 1411 and continued to be used throughout American history. In 1878, Southern Democrats angry about Reconstruction policies gained Congressional control. They enacted what became known as the *Posse Comitatus* Act which criminalized using the Army or Air Force to execute laws unless expressly permitted by the Constitution or statute. That act now is 18 *US Code* §1385, which causes much confusion among military services regarding its application.[44] Subsequently, 10 *US Code* §275 restricts members of the Navy from "direct participation … in a search, seizure, arrest,

[44] Matt Matthews, *The Posse Comitatus Act and the United States Army: A Historical Perspective* (Fort Leavenworth, KS: Combat Studies Institute Press, 2006), 1-46; Banks and Dycus, 92-93, 105-112; US CRS, *The Posse Comitatus Act and Related Matters: The Use of the*

or other similar activity unless participation in such activity by such member is otherwise authorized by law."[45] The plain text of 10 *US Code* §275 is silent about whether it includes the USCG when it operates as part of the Navy.[46]

Further, the more recent Homeland Security Act reaffirms "the continued importance of [18 *US Code* §1385] … in [restricting] any use of the Armed Forces as a *posse comitatus* to execute the laws."[47] This provision's broader use of "Armed Forces" than 18 *US Code* §1385's "the Army or the Air Force" further adds to the confusion for the USCG since 14 *US Code* §1 defines the USCG as "a military service and a branch of the armed forces of the United States at all times." As previously detailed, the USCG is responsible for law enforcement and assisting in law enforcement. Additionally, one statute specifically authorizes the USCG to assist "any Federal agency, State, Territory, possession, or political subdivision thereof, or the District of Columbia, to perform any activity for which such personnel and facilities are especially qualified" when requested by the proper authority.[48] Thus, it seems logical that the USCG is exempted from the limits on the use of *posse comitatus* and on the military for direct participation in law enforcement. Otherwise, many statutorily authorized and mandated USCG missions are defeated. The plain text of the statutes could cause confusion, especially in a crisis or multi-

---

Military to Execute Civilian Law, by Charles Doyle and Jennifer K. Elsea, R42659 (Washington, DC, August 16, 2012), 19-20, accessed February 5, 2017, https://fas.org/sgp/crs/natsec/R42659.pdf.

[45] National Defense Authorization Act for Fiscal Year 2017, Public Law 114-328, div. A., title XII, §1241(a)(2), *US Statutes at Large* 130 (2016): 2497, codified at *US Code* 10 (2017), §275 (renumbered 50 *US Code* §375 to §275).

[46] US CRS, *The Posse Comitatus Act and Related Matters*, 4. USCG is not mentioned in the *posse comitatus* prohibitions, and "[a]s a practical matter, however, the USCG is statutorily authorized to perform law enforcement functions." Banks and Dycus, 110. These authors take the view that the USCG "is subject to the *Posse Comitatus* Act only when it is called into service as part of" the US Navy.

[47] *US Code* 6 (2017), §466.

[48] *US Code* 14 (2017), §141.

faceted, evolving operation. In at least one documented instance, a USCG judge advocate general believed the USCG violated the *posse comitatus* prohibition when called upon to assist in the DC sniper hunt that terrorized the metropolitan area of the nation's capital for months and resulted in multiple deaths.[49]

Chemical Sector

The statutory authority for the CFATS Program expires in December 2018 unless reauthorized by law.[50] Also, it only covers establishing performance standards. One report questioned whether the program should augment its performance-based approach with prescriptive regulations.[51] Finally, the program, while making great strides in improving the security of chemical facilities, has problems with non-compliant facilities.[52] In the plant explosion in West, Texas in 2013, the facility failed to report its ammonium nitrate holdings to the CFATS Program. The final report investigating the explosion noted that if the facility "had complied with the CFATS [Program], a CFATS [Program] inspection or assistance visit might have noted the storage conditions … and prompted change."[53]

---

[49] Banks and Dycus, 194-195, citing Elaine M. Grossman, "Former JAG: Military Aid in DC Sniper Pursuit May Have Broken Law," *Inside the Pentagon*, Inside Washington Publishers, November 14, 2002, accessed April 4, 2017, https://fas.org/sgp/news/2002/11/itp111402.html.

[50] Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014, Public Law 113-254, *US Statutes at Large* 128 (2014): 2919, set forth in note following *US Code* 6, §621.

[51] US CRS, *Issues in Homeland Security Policy for the 113th Congress*, 22.

[52] US DHS, NPPD, *Statement for the Record of Assistant Secretary Caitlin Durkovich, NPPD, and Director David Wulf, NPPD, before the Committee on Homeland Security, US House of Representatives* (Washington, DC, February 27, 2014), accessed March 23, 2017, http://docs.house.gov/meetings/HM/HM08/20140227/101787/HHRG-113-HM08-Wstate-DurkovichC-20140227.pdf.

[53] US Chemical Safety and Hazard Investigation Board, *Investigation Report: West Fertilizer Company Fire and Explosion (15 Fatalities, More than 260 Injured), West, TX April 17, 2013, Final Report 2013-02-I-TX* (Washington, DC, January 2016), 55, 175, accessed March 5, 2017, http://www.csb.gov/west-fertilizer-explosion-and-fire-/. Fifteen people were killed, more than 260 people injured, and many required hospital admission. The fertilizer, blending, retail,

Conclusion

The Homeland Security Act offers limited authority for the DHS to establish protective standards or to physically protect and secure critical infrastructure where an owner fails to adequately protect it. For example, the GAO acknowledged the DHS has no authority to set standards for the electrical grid which affects every other critical infrastructure sector.[54] USCG authority related to critical infrastructure is not explicit and is limited in some areas to emergency or wartime. Also, the question of the *posse comitatus* limitation could cloud USCG operational effectiveness. The DHS can exercise its statutory authority to influence the infrastructure owners and other government agencies with regulatory authority over infrastructure security;[55] to exercise its limited areas of regulatory and statutory authority to protect government property and ports, waters, and coastline; and to exercise its defined regulatory authority over certain chemical facilities and certain ammonium nitrate transactions. The DHS, however, has no statutory authority for strategic, integrated regulation of minimal standards or of physically protecting critical infrastructure where an owner fails to implement protective measures or inadequately protects the infrastructure.

---

and distribution facility was completely destroyed, with widespread damage to more than 150 offsite buildings, including residences, schools, and other structures. More than half of the damaged structures had to be demolished and reconstructed, including schools, an apartment building, and a nursing home. Total loss was estimated at $230 million. Federal disaster assistance was estimated to exceed $16 million. The company was insured for one million dollars and declared bankruptcy.

[54] US GAO, *Critical Infrastructure Protection: DHS Has Made Progress in Enhancing Critical Infrastructure Assessments*, 10.

[55] *US Code* 6, §121. The OIP has statutory authority to assess and make recommendations about critical infrastructure and to collect, analyze, and share information about critical infrastructure protection and threats.

Section Five: Existing Federal Statutory Authority for the DOD

The DOD has no regulatory authority relevant to critical infrastructure protection. Its federal statutory authority for physical protection and security is limited. Title 32 authorizes the DOD to fund National Guard protection of critical infrastructure. Multiple authorities authorize the DOD, under specific statutorily defined circumstances to act in support of civilian authorities. Like the DHS, the DOD has challenges in exercising its authority which could leave critical infrastructure unprotected and vulnerable, thereby compromising the DOD's ability to fulfill this national security goal.

Key Task: Standards—Establishing Standards and Enforcing Compliance

The DOD has no statutory authority to establish standards to guide critical infrastructure protection.

Key Task: Security—Physically Protecting and Securing Critical Infrastructure

The authority for the DOD to physically protect and secure critical infrastructure either routinely or in an emergency derives from Titles 32, 10, 14, and 42. Title 32 provides the clearest authority by permitting DOD funding for the National Guard to perform homeland defense duties, specifically including critical infrastructure protection. Title 10 authorizes use of military forces for specific situations to restore law and order, to enforce federal authority, and to enforce federal and state law, including assisting the Department of Justice (DOJ). Title 14 USCG personnel are available. Finally, the DOD may assist in emergency situations if the president invokes Title 42 for disaster/emergency assistance. The table below lists authorized use of military service members within the US homeland:

Table 5. Authorized Use of the Military within the United States

US Code	Reason/Circumstance	Condition/Determination	Deploy
32 *USC* §904	Homeland defense duty, including military protection of critical infrastructure	Secretary of Defense determines critical to national security	Funding for National Guard
10 *USC* §251	Aid state to suppress insurrection	State legislature or governor requests aid from the president	Militia of other state
10 *USC* §252	Enforce federal authority	President determines that (1) unlawful obstruction, combination, or assemblage or rebellion (2) impractical to enforce US laws through judiciary	Militia of any state
10 *USC* §253	Enforce federal or state law	President determines that (1) necessary to suppress insurrection, domestic violence, unlawful combination, or conspiracy; and (2) either (a) it hinders execution of law so that people are deprived of a constitutional right and state does not protect or (b) it opposes or obstructs execution of law or impedes justice under law	Militia, armed forces, or both
10 *USC* §282	Emergency involving weapon of mass destruction	Secretary of Defense upon request of Attorney General to assist DOJ	DOD personnel
10 *USC* §283	Bombings of places of public use, government facilities, public transportation and infrastructure facilities	Secretary of Defense upon request of Attorney General to assist DOJ	DOD personnel
10 *USC* §284	Support for counter drug and counter transnational organized crime activities	Secretary of Defense may provide support to any federal entity or state, local, tribal, or foreign law enforcement agency	DOD personnel, specified support
10 USC §10102	War, national emergency, and as national security may require	Augment regular forces with reserve components	Reserves
10 USC §12406	Invasion or rebellion or danger of; execute US laws	National Guard called to federal service if regular forces insufficient	Regular, National Guard
Title 14 *USC*	Coast Guard	Title 14 authority; operate in US Navy when designated	USCG
46 *USC* §5170, §5191	Natural disaster, emergency	President may deploy, either with or without request of state governor	DOD personnel

Source: Author created. Some of these sections are renumbered from law in effect prior to December 23, 2016. The National Defense Authorization Act for Fiscal Year 2017, Public Law 114-328, div. A, title XII, §1241(a)(1) and (2), *US Statutes at Large* 130 (2016): 2497, codified at *US Code* 10 (2017), §§251-255 (chapter 13, Insurrection) (previously §§331-§335 (chapter 15, Insurrection)) and at *US Code* 10 (2017), §§271-283 (chapter 15, Military Support for Civilian Law Enforcement Agencies) (previously §§371-383 (chapter 18, Military Support for Civilian Law Enforcement Agencies). This law added *US Code* 10 (2017), §284 (military support to counter drugs and transnational organized crime).

National Guard, Title 32

The most explicit statutory authority is Title 32 funding authority for "homeland defense activity" which includes military protection of critical infrastructure. The DOD may fund state National Guard forces to perform "the military protection … of infrastructure or other assets of the United States determined by the Secretary of Defense as being critical to national security, from a threat or [an] aggression."[56] This authority would address routine and emergency protection and security.

Armed Forces and National Guard, Title 10

In addition, physically protecting and securing critical infrastructure could be part of restoring law and order, enforcing federal authority, or enforcing federal or state law. One statute authorizes the president, upon request of the state's legislature or governor if the legislature cannot be convened, to call into federal service the militia of another state and "use such of the armed forces, as [the president] considers necessary to suppress the insurrection."[57] Another statute authorizes the president to use militia of any state to enforce US law or suppress rebellion where "unlawful obstructions, combinations, or assemblages, or rebellion against the authority of the United States, make it impractical to enforce the laws of the United States in any State by the ordinary course of judicial proceedings…."[58] A third statute authorizes the president "by using the militia or the armed forces, or both, or by any other means shall take such measures as [the president] considers necessary to suppress, in a State, any insurrection, domestic violence, unlawful combination, or conspiracy." This statute applies where (1) violence or unlawful activity

[56] Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005, Public Law 108-375, div. A, title V, §512(a)(1), *US Statutes at Large* 118(2004): 1811, codified at *US Code* 32 (2017), §§901-908.

[57] *US Code* 10 (2017), §251.

[58] *US Code* 10 (2017), §252.

hinders the execution of state law or federal law within the state and deprives people of a "right, privilege, immunity, or protection named in the Constitution and secured by law" and (2) the state authorities "are unable, fail, or refuse" protection or the disturbance "opposes or obstructs the execution of federal law or impedes the course of justice under those laws."[59] Finally, reserve and National Guard forces may be activated: (1) reserves – upon war, national emergency, national security requirements; and (2) National Guard – upon actual or danger of invasion or rebellion against US authority and to execute US law when the president "is unable with the regular force to execute the laws of the United States."[60] The president could order critical infrastructure to be physically protected and secured as a necessary action pursuant to these statutes.

Also, the DOD has statutory authority to support DOJ activities to enforce laws related to bombings, biological and chemical weapons, and weapons of mass destruction (WMDs). The statute related to bombings authorizes the DOD to support the DOJ in enforcing the law that prohibits bombings of infrastructure facilities, public transportation systems, state or government facilities, and places of public use. The action must be necessary for "the immediate protection of human life and civilian law enforcement officials are not capable of taking the action."[61] The statutes related to biological and chemical weapons and WMDs authorize the DOD to assist the DOJ in emergency situations in enforcing laws that prohibit weapons of mass destruction.[62] Both

[59] *US Code* 10 (2017), §253.

[60] *US Code* 10 (2017), §§10102, 12406.

[61] *US Code* 10 (2017), §283(a); *US Code* 18 (2016), §2332f.

[62] *US Code* 10 (2017), §282. “The Secretary of Defense, upon the request of the Attorney General, may provide assistance in support of Department of Justice activities relating to enforcement of section 175, 229, or 2332a of title 18 during an emergency situation involving a weapon of mass destruction.” *US Code* 10 (2017), §283(b). “Military explosive ordnance disposal units providing rendering-safe support to Department of Justice activities relating to the enforcement of section 175, 229, or 2332a of title 18 in emergency situations involving weapons of mass destruction shall provide such support in a manner consistent with the provisions of section 328 of this title.” *US Code* 18 (2017), §175, biological weapons; *US Code* 18 (2017), §229, chemical weapons; *US Code* 18 (2017), §2332a, weapon of mass destruction.

statutes require the Attorney General to request DOD assistance and are limited to emergency situations. Physically protecting and securing critical infrastructure is not mentioned specifically in either statute.

Coast Guard, Title 14

The USCG at all times is a military service. It serves the DHS, except when it operates as a service to the US Navy either upon a Congressional declaration of war or when the president directs.[63] The statutory authority for the USCG is discussed in section four. For purposes of the analysis in this section, the USCG has explicit statutory authority to engage in law enforcement activity and to protect US ports, waters, and coastline, either separately or in concert with the Navy.

Disaster Relief and Emergency Assistance, Title 42

Finally, the president has authority in a natural disaster or an emergency to deploy any federal agency, both with and without the request of a state governor. This authority could include directing the DOD to physically protect and secure critical infrastructure. A state governor may request assistance in a major disaster or emergency.[64] The president may direct federal support of state and local assistance response or recovery efforts.[65] The president also may

[63] *US Code* 14 (2017), §1 and §3.

[64] Robert T. Stafford Disaster Relief and Emergency Assistance Act, Public Law 100-707, *US Statutes at Large* 102 (1988):4696, codified at *US Code* 42 (2017), §5170(a), (b), major disaster; §5191(a), (c), emergency assistance. Both statutes also permit a request by an Indian tribal chief executive. *US Code* 42 (2017), §5122. A "major disaster" is a natural catastrophe (including hurricane, tornado, tsunami, snowstorm, drought, etc.) "or, regardless of cause, any fire, flood, or explosion" that the president determines "causes damage of sufficient severity and magnitude to warrant major disaster assistance…" An "emergency" means "any occasion or instance for which, in the determination of the President, Federal assistance is needed to supplement State and local efforts and capabilities to save lives and to protect property and public health and safety, or to lessen or avert the threat of a catastrophe in any part of the United States."

[65] *US Code* 42 (2017), §5170a, major disaster assistance; §5191(a), emergency assistance.

act without a request from the governor in a major disaster or emergency, "where necessary to save lives, prevent human suffering, or mitigate severe damage;" in a major disaster, where "essential to meeting immediate threats to life and property," or to provide emergency communication systems or emergency public transportation or fire management assistance; and in an emergency, where the federal government has primary responsibility for response because under the Constitution or federal statutory law the federal government exercises exclusive or preeminent responsibility and authority over the subject area.[66] It is reasonable to conclude that the President would deem physically protecting and securing critical infrastructure as mitigating severe damage or essential to meeting a threat to life or property.

Challenges for the DOD in Exercising This Statutory Authority

Whether Title 32, 10, 14, or 42 is invoked, or a combination thereof, the DOD has multiple challenges in unequivocally exercising its authority. These challenges could compromise the orderly and predictable physical protection and security of critical infrastructure.

National Guard, Title 32

First, the Title 32 statutory framework assumes that the state governor and the DOD will agree on the mission, threat assessment, and scope. It also assumes that the state governor will agree with the amount of DOD funding and proceed with the mission.[67] A second assumption is

[66] Major disaster and emergency: *US Code* 42 (2017), §5170a(5) and §5191(b)(5), "where necessary to save lives, prevent human suffering, or mitigate severe damage." Major disaster: *US Code* 42 (2017), §5170b, "essential to meeting immediate threats to life and property;" §5185, emergency communications systems, including before disaster; §5186, emergency public transportation; §5187, fire management assistance. Emergency: *US Code* 42 (2017), §5191(b), the federal government has primary responsibility for response because of exclusive or preeminent responsibility and authority pursuant to the Constitution or federal law.

[67] *US Code* 32 (2017), §905. The Secretary of the DoD provides funds "to that State in an amount that the Secretary determines is appropriate." This clarity, however, does not mean the State must accept the mission or the amount of funding determined by the DoD.

that the state National Guard has the capability and personnel available for the homeland defense activity identified by the DOD or requested by the governor, especially considering the duty is limited to one hundred and eighty days.[68] Finally, this authority requires the DOD to engage in additional recordkeeping, auditing, and compliance monitoring.[69]

Armed Forces and National Guard, Title 10

The most confusing challenge to exercising Title 10 authority may be the limitations placed upon the *posse comitatus* doctrine. Some Title 10 statutes specifically authorize military support to law enforcement related to weapons of mass destruction (WMD) and bombings. Similar to the initial confusion on 9/11 as to the "cause" of the disaster/emergency/crisis, a circumstance may require military support even before determining whether the triggering event was a WMD or a bombing.[70] Further, some statutes have specific exceptions, such as "for the immediate protection of human life, and civilian law enforcement officials are not capable of taking the action."[71] State National Guard units, except ones that are federalized, and the USCG, possibly except when operating as part of the Navy, are exempt from the bar against *posse comitatus* activity.[72] This situation may lead to not federalizing National Guard units to avoid the

[68] *US Code* 32 (2017), §904(b). The statute limits this duty to 180 days. The time may be extended once for 90 days “to meet extraordinary circumstances.”

[69] *US Code* 32 (2017), §906. The statute requires specific reporting to Congress. Also, a funding request initiated by the governor must contain a certification that homeland defense activities “are to be conducted at a time when the personnel involved are not in Federal service.”

[70] Also, consider the case of an EMP burst, which studies predict would result in widespread devastation and chaos that likely will completely overwhelm state and local first responders. Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack; Sirius Bontea, “America’s Achilles Heel: Defense Against High-Altitude Electromagnetic Pulse: Policy v. Practice” (master’s thesis, US Army Command and General Staff College, 2014), accessed March 5, 2017, http://www.dtic.mil/docs/citations/ADA613532.

[71] *US Code* 10 (2017), §274, §275, §282, §283. *US Code* 10 (2017), §282, §283.

[72] *US Code* 10 (2017), §275, specifies “Army, Navy, Air Force, or Marine Corps;” *US Code* 18 (2017), §1385, specifies “Army or Air Force.”

confusion at times when they need to be federalized for operational effectiveness. The military has multiple branches and engages in joint planning, training, and operations, including with the National Guard and the USCG. Navigating the statutory authorizations, prohibitions, limitations, and exceptions related to *posse comitatus* is like a maze.[73]

Coast Guard, Title 14

The USCG is a hybrid force: a military service and branch of the armed forces, as well as a law enforcement authority. As discussed in section four, interpreting and applying *posse comitatus* limitations to the USCG present a challenge, especially when the USCG may be transferred to the US Navy where its operations may be changed to synchronize with Navy operations.[74]

Disaster Relief and Emergency Assistance, Title 42

The statutory framework for disaster response and emergency assistance and recovery has at least two challenges. A most daunting challenge involves the dual command problem where National Guard forces have a separate command chain than federal forces, including federalized National Guard forces, military active duty forces, and federal disaster response and law enforcement personnel, as illustrated by this graphic:

[73] US CRS, *The Posse Comitatus Act and Related Matters*, 30. This report prepared for Congress lists twenty-two statutory exceptions to the *Posse Comitatus* Act. This CRS list does not include, however, 10 *US Code* (2017), §§271-284, some of which contain additional exceptions to the *posse comitatus* prohibition. Banks and Dycus, 103, 193-195.

[74] *US Code* 14 (2017), §3(b).

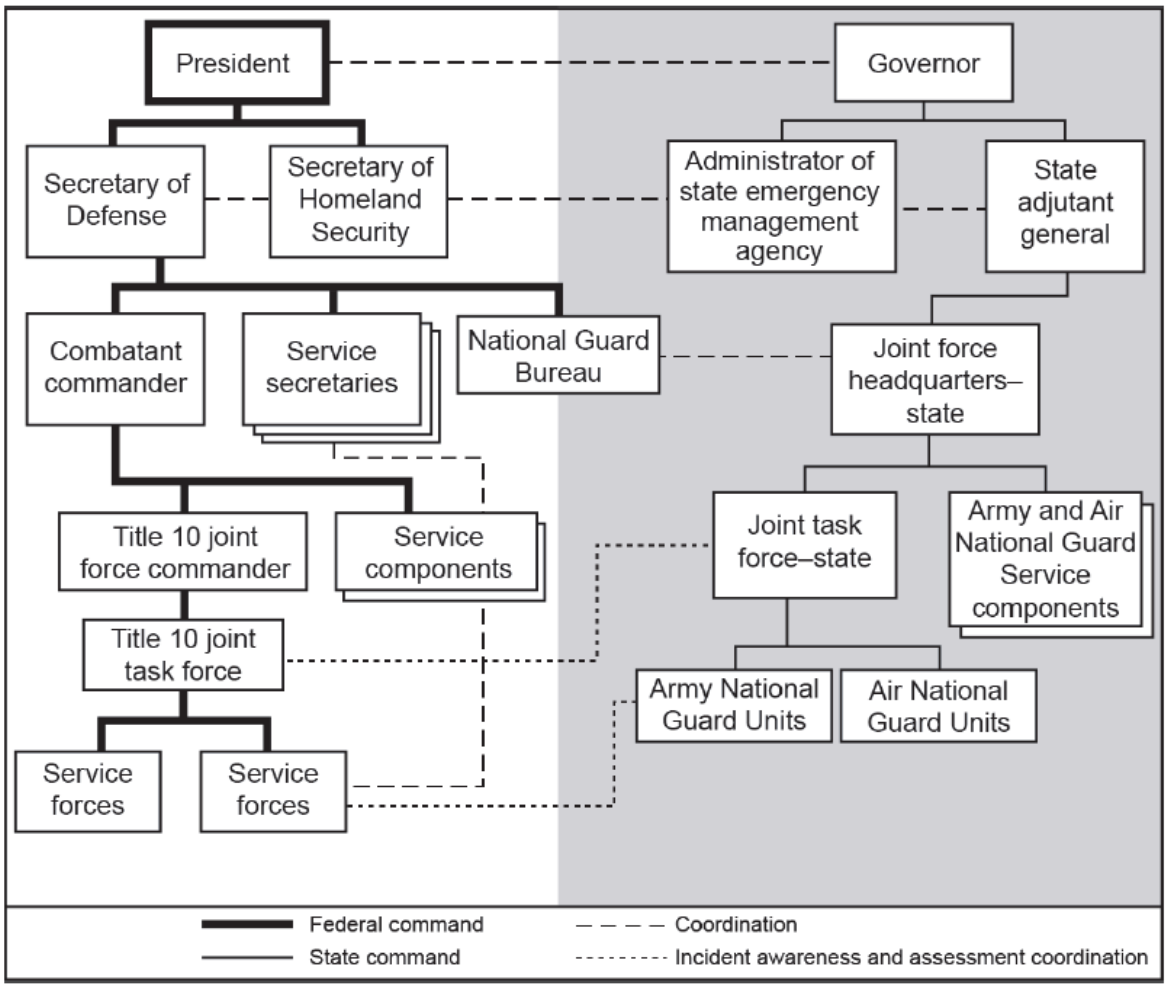

Figure 1. Dual/Parallel Command Structure with Federalized State National Guard. US DOD, Department of the Army, Headquarters, *ADRP 3-28, Defense Support of Civil Authorities*, 3-9 (Figure 3-5. Example of parallel command structure).

The governor of a state may mitigate the parallel command challenge by agreeing to appointment of a dual status commander, as illustrated below:

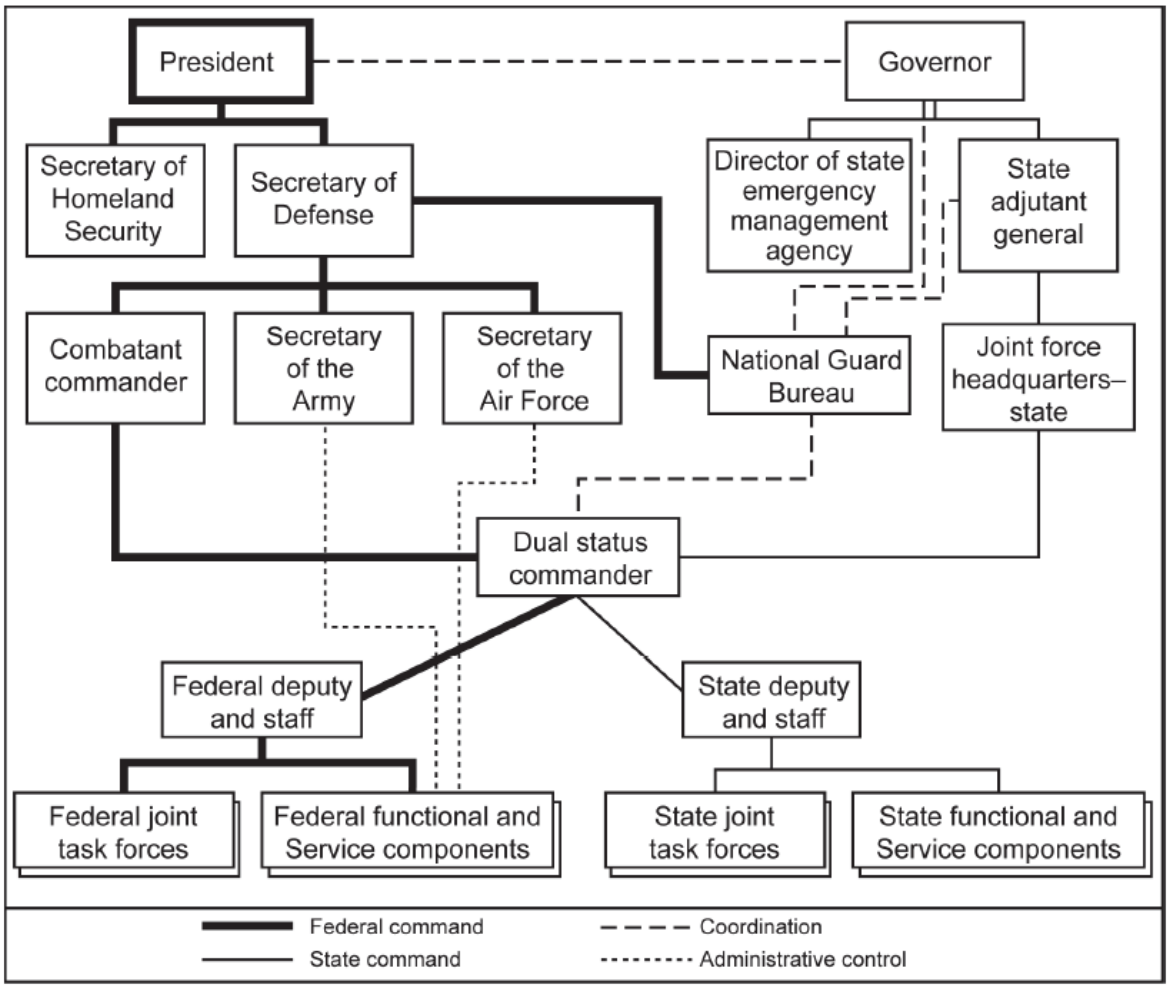

Figure 2. Dual Status Command Solution with Federalized State National Guard. US DOD, Department of the Army, Headquarters, *ADRP 3-28, Defense Support of Civil Authorities*, 3-10 (Figure 3-6. Example of dual-status command structure).

However, nothing in federal law requires the governor to agree to appointment of a dual status commander.

In addition, arbitrary distinctions as to the cause of the emergency drive the types of action: (1) between "major disaster" and "emergency" and (2) between actions authorized after a governor requests assistance and actions authorized based upon a presidential determination. It seems that a catastrophe is an emergency regardless of whether caused by a brutal hurricane, raging fire, devastating explosion triggered by human error or an explosion or bomb detonated by a criminal or terrorist, or a nuclear or EMP attack. For example, if a governor requests assistance,

the disaster relief assistance includes "precautionary evacuations and recovery" and "recovery activities, including disaster impact assessments and planning." However, emergency assistance without a governor's request does not include these actions.[75] An emergency response may require some precautionary evacuations (for example, clearing a bomb site or suspected bomb site locale) and recovery efforts. These statutorily defined and overlapping categories, that seem arbitrary, may unnecessarily complicate operationalizing crisis planning and response, especially in joint environments and in major crises (the very ones that require swift, decisive response).[76]

Conclusion

No statutory authority authorizes the DOD to regulate to set standards for critical infrastructure protection. That lack of authority is appropriate for our civilian government, so that a purely civilian department exercises regulatory authority in such matters. The DOD has statutory authority which would encompass physically protecting and securing critical infrastructure if an owner does not adequately do so. This authority applies only in certain circumstances. Challenges in exercising these authorities could exacerbate crisis response and could compromise DOD's ability to perform this task as effectively as needed.

---

[75] *US Code* 10 (2017), §5170a(2), “including precautionary evacuations and recovery,” and §5170a(3)(F), “recovery activities, including disaster impact assessments and planning,” compared with §5191(b)(2) and (3).

[76] US DHS, USCG, *BP Deepwater Horizon Oil Spill: Incident Specific Preparedness Review (ISPR), Final Report* (Washington, DC, January 2011), 9, accessed January 21, 2017, http://www.uscg.mil/foia/docs/DWH/BPDWH.pdf. The USCG report on the 2010 Deepwater Horizon disaster noted confusion by state and local authorities. State and local authorities were familiar with the National Response Framework (NRF) used for hurricanes and similar disasters. An oil well explosion and massive oil spill, however, is not one of the NRF planning scenarios so response proceeded instead under the National Contingency Plan.

Section Six: Implications for National Security and Critical Infrastructure Protection

Three conclusions are evident from the analysis of this survey of federal statutory law, including where an owner fails to adequately protect the infrastructure. These conclusions identify ways in which the federal statutory framework offers insufficient authority for the DHS or the DOD, acting separately or jointly, to achieve the national security goal of protecting critical infrastructure. This analysis demonstrates the need to strategically review previous policy assumptions about the public-private partnership model where the private sector implements action to yield protected critical infrastructure. In addition, two specific areas may be addressed by targeted statutory action to address the confusion around the *posse comitatus* doctrine and to remedy the dual command problem. US policy has long favored an integrated national security policy. It appears that critical infrastructure protection, even from this brief, targeted survey, is anything but integrated.

Strategic Analysis and Policy Considerations

Three Conclusions

Three conclusions are relevant to national strategic policy for protection of critical infrastructure, including as owned by private and non-federal government entities that fail to adequately protect it:

(1) the DHS regulatory authority to set standards is very limited and the DHS has no integrated, strategic authority to set even minimal standards for critical infrastructure protection, even where another agency has no relevant authority or does not exercise its authority;

(2) the DHS and the DOD federal statutory authority to physically protect and secure critical infrastructure routinely and in an emergency is limited and lacks integration; and

(3) no statute defines how the DHS and the DOD are to work together to achieve the national security goal of critical infrastructure protection, even in an emergency or a crisis.

Strategic Review for Integrated National Security and Critical Infrastructure Protection

These deficiencies and others suggested by this survey present the need for a strategic review to integrate national security and critical infrastructure protection policy. The United States previously has moved to integrate national security policy. In 1947, Congress articulated the need for integrated, comprehensive, and strategic US security; unified direction, authority, and control under civilian control; "more effective, efficient, and economical administration"; and elimination of "unnecessary duplication … particularly in the field of research and engineering."[77] The 1947 National Security Act consolidated the military and defense services into the DOD. In 1986, Congress reorganized and streamlined the DOD to establish clear authority, responsibility, and chain of command; to achieve integration and synthesis of the various capabilities of the military services; "to improve the military advice provided to the President"; "to increase attention to the formulation of strategy and to contingency planning"; and "to provide for more efficient use of defense resources."[78]

Today, the DHS has the homeland security mission to protect the nation from terrorism and to respond to disasters and emergencies, and the DOD has the homeland defense mission, terrorism fight, support for disasters and emergencies, and support to civilian law enforcement agencies. Neither department has federal statutory authority for an integrated plan or response to critical infrastructure protection. For example, neither department can effectuate a solution such as for electric grid owners who fail to adopt available security measures or chemical facility owners who fail to avail themselves of available resources that may have prevented deadly and

[77] The National Security Act of 1947, Public Law 114-328, chapter 343, §2, *US Statutes at Large* 61 (1947): 496, subsequently amended, and codified at *US Code* 50 (2017), §3002.

[78] Goldwater-Nichols Department of Defense Reorganization Act of 1986, Public Law 99-433, *US Statutes at Large* 100 (1986): 992 *et seq.* and 993-994 (policy), codified at *US Code* 10 (2017), §101 *et seq*., and policy set forth at *US Code* 10 (2017), §111 note.

costly infrastructure catastrophes.[79] The DHS statutory authority authorizes studying, assessing, sharing information, and reporting to stakeholders and Congress about critical infrastructure protection needs and mandates building a national asset database.[80] A strategic review could work to resolve the limits to the DHS regulatory authority to set minimal standards for critical infrastructure protection as a guide so that owners who are not protecting infrastructure at least would be required to meet some minimal threshold. This measure is especially important for integrated and regional or nationwide critical infrastructure, such as the electric grid and emergency services, and especially where no federal agency has regulatory authority for security or does not exercise its authority. Also, a strategic review could address gaps in the ability of the DHS and/or the DOD to physically secure critical infrastructure where an owner fails to adequately do so. Finally, a strategic review could define how the DHS and the DOD work together, especially in a crisis, which would facilitate joint training and exercises.[81]

The limited authority of the DHS contrasts starkly with its broad statutory mission with grave national consequences: to "prevent terrorist attacks," "reduce the vulnerability … to terrorism," and "minimize the damage … from terrorist attacks that do occur" within the United

---

[79] See earlier discussion of attacks on the electric grid in Metcalf, CA and the explosion in West, TX.

[80] *US Code* 6 (2017), §121(d), §124l.

[81] *US Code* 6 (2017), §456. US CRS, *Defining Homeland Security*, Summary. This report cautions that "the US government does not have a single definition for 'homeland security' … [which] may impede the development of a coherent national homeland security strategy and may hamper the effectiveness of Congressional oversight." Banks and Dycus, 11, 265, 274-75. These authors conclude: "Civilian agencies, chiefly the Department of Homeland Security, should harmonize their emergency response plans with those of the Defense Department, including the establishment of a single line of command authority." US CRS, *Issues in Homeland Security Policy for the 113th Congress*, 1, 3. This CRS report states that several homeland security functions remain with "their original executive branch agencies and departments, including the Departments of Justice, State, Defense, and Transportation." The report cautions: "Without a general consensus on the literal and philosophical definition of homeland security, achieved through a strategic process, some believe that there will continue to be the potential for disjointed and disparate approaches to securing the nation."

States and to protect critical infrastructure.[82] Yet the policy assumption in the CIPA and PPD-21 rests upon non-federal infrastructure owners acting in partnership with the federal government. As aptly noted with respect to the electric grid, the interconnected, networked nature of critical infrastructure that crosses over state and local jurisdictions may make this public-private partnership paradigm – as the only framework – unrealistic for national security.[83] Second, the diffusion of regulatory authority among discrete DHS entities and among multiple federal departments and agencies hobbles an integrated approach. The DHS has no regulatory authority to set minimal national standards, to compel agencies with regulatory authority to issue protection standards, or to act in that agency's stead. Further, the DHS has no authority to compel that information be provided and updated for the national asset database and prioritized critical infrastructure list required by the Homeland Security Act.[84]

Physical protection is crucial with widespread disasters or in the face of credible threats of coordinated terrorist action against key critical infrastructure such as water and dams or the electric grid. If state and local law enforcement authorities are overwhelmed or lack the capacity to physically protect and secure the infrastructure, the DHS and the DOD statutory framework must be clear as to authority and responsibilities, including unified command authority.[85]

---

[82] *US Code* 6 (2017), §§111(b)(1), 121(d).

[83] Hayes and Ebinger, 1-2, 19-20. Study results indicate that the private sector is focused on day-to-day vandalism and theft threats and believes that "the government will step in to cover losses in the event of a catastrophe." ICF International, 88.

[84] *US Code* 6 (2017), §124, national asset database, prioritized list. US GAO, *Critical Infrastructure Protection: Observations on Key Factors in DHS's Implementation of Its Partnership Approach, Testimony Before the Committee on Homeland Security and Governmental Affairs, US Senate*, by Stephen L. Caldwell and Gregory C. Wilshusen, GAO-14-464T (Washington, DC, March 26, 2014), 6, accessed March 12, 2017, http://www.gao.gov/assets/670/661945.pdf. This report notes that industry does not want to share information with the federal government and opines that the government needs to collect information about why facilities did not make security-related improvements.

[85] Examples are in sections four and five of this paper, in addition to the 2010 Deepwater Horizon disaster report that noted confusion by state and local authorities. US DHS, USCG, *BP Deepwater Horizon Oil Spill: ISPR*, 9.

How to accomplish a strategic review? Consider forming a commission to analyze and recommend strategic policy and tactical implementation options for protecting critical infrastructure, including how to address the reality of non-federal infrastructure owners who fail to adequately protect critical infrastructure. Primary considerations should be the representativeness and legitimacy of the commission. Members should be representative of the relevant issues and diverse in views with no vested interest, other than as dedicated, concerned Americans. Examples of members could include: retired members of the public, including state and local government officials, non-government entities, private owners, first responders, and concerned citizens; retired members of the US Congress, courts, military services, and federal government departments; and a limited number of retired military service members, including general and field officers and enlisted members. Champion legitimacy by having the fact-deciders and recommenders not have a profit, promotion, or reelection stake in the data collection, analysis, or recommendations. A second consideration is building or creating the political will to tackle the issues and recommendations rather than defaulting to the *status quo*. Congress must be committed to act on reasoned recommendations to secure our nation's critical infrastructure, rather than reacting to the next crisis.

Two Specific Considerations

In the nearer term, two specific challenges could be addressed by new statutory law.

Posse Comitatus and Criminal Penalties

The doctrine of *posse comitatus* and attempts to limit it have created confusion and clouded the military's effective response to domestic emergencies, including in Katrina in 2005 and in the Los Angeles riots in 1992.[86] One of the reports from Katrina recommended revisiting

[86] Banks and Dycus, 91-92, 105-106.

this issue.[87] The statute enacted in a 2006 post-Katrina response was repealed shortly thereafter upon complaints from the Council of Governors about inadequate consultation.[88] The Katrina recommendation, therefore, remains unaddressed. More recent authors also have called for revisiting this issue. [89]

The original 1878 *Posse Comitatus* Act, currently in 18 *US Code* §1385, should be repealed. The original 1878 *Posse Comitatus* Act, enacted to thwart federal post-Civil War reconstruction and integration efforts, was moved to the US criminal code in 1956.[90] It is an unnecessary remedy that has stifled responses in the past and that could stifle or chill authorized action in a crisis. The confusion could create cascading delays, for example, in light of more recent statutory law specifically authorizing military support of law enforcement and in the hybrid nature of the USCG.

The strategic review of national security policy then could address overarching policy considerations as to the authorized use of the military in the homeland. The strategic review also could consider whether any streamlining and clarity of statutory law is necessary or would be helpful to clarify the various statutes that bar the military from direct participation in law enforcement "unless otherwise authorized by law."[91]

---

[87] The White House, 54-55.

[88] Banks and Dycus, 107-108; US CRS, *The Posse Comitatus Act and Related Matters*, 1.

[89] Banks and Dycus, 275. The way the *posse comitatus* doctrine has evolved in the United States needs to be reexamined and "possibly adjusted to enable a practical, response flexible response to future black swans and other crises. Deborah L. Geiger, "*Posse Comitatus*, the Army, and Homeland Security: What is the Proper Balance?" (strategy research project, US Army War College, 2006), accessed April 2, 2017, https://www.hsdl.org/?view&did=469535. This author reviews the history of *posse comitatus* and proposes allowing trained military police personnel to assist more actively civilian law enforcement personnel in response to domestic emergencies.

[90] *US Code* 18 (2017), §1385, previously was in Title 10 but was moved to Title 18 (Crimes) in 1956. *US Statutes at Large* 70A (1956): 626.

[91] *US Code* 10 (2017), §275 (DoD); *US Code* 6 (2017), §466 (DHS); US CRS, *The Posse Comitatus Act and Related Matters*, 30; Banks and Dycus, 103, 193-195; statutes listed in Table 5 in section five of this paper.

Dual Command Problem and the Need for Unified Command

The provision of federal assistance could be conditioned upon using the dual status command model. Such a construct provides input from a state directly into the chain of command while also preserving operational fidelity and the president's constitutional command authority over the US military.

Concluding Thoughts

Conducting a strategic review is a much needed opportunity to examine national security policy and critical infrastructure protection, as well as embedded policies about the functions of homeland security, homeland defense, and disaster/emergency preparedness and response. The Constitution is clear about the exclusive and preeminent authority and responsibility for national security and national defense being the province of the federal government where Congress is:

> … [to] provide for the common Defence and general Welfare of the United States;
>
> ... to provide for calling forth the Militia to execute the Laws of the Union, suppress Insurrections and repel Invasions;
>
> … to provide for organizing, arming, and disciplining, the Militia, and for governing such Part of them as may be employed in the Service of the United States, reserving to the States respectively, the Appointment of the Officers, and the Authority of training the Militia according to the discipline prescribed by Congress.[92] (emphasis added).

When the United States calls forth the militia (now the National Guard) to execute the laws of the Union, the militia should be in the service of the United States.[93] In addition, the regular US military forces (non-National Guard) are authorized by statutory law to act domestically in certain

[92] US Constitution, preamble and art. 1, sec 8.

[93] *US Code* 10 (2017), §12406. The National Guard may be activated to federal service where invasion or danger of invasion; rebellion or danger of rebellion against US authority; or "the President is unable with the regular forces to execute the laws of the United States." US CRS, *The Posse Comitatus Act and Related Matters*, 30. This CRS report lists this statute as a statutory exception to the *Posse Comitatus* Act.

circumstances.[94] These circumstances can include physically protecting and securing critical infrastructure.

Americans in an emergency may not care so much about the color of the uniform the person is wearing who protects a nearby major dam or electrical grid component or plucks them from the rooftops of their hopelessly flooded neighborhoods, secures them against wanton opportunistic or criminal violence, delivers life-saving clean water and emergency food, or takes them to a secure shelter. For all of the separate and overlapping statutes and policy discussions, it may not matter whether the person's uniform is the green, blue, tan, or white of the US military or black, blue, green, gray, tan, red, or yellow of state or local law enforcement or emergency responders and whether the securer, defender, or responder acts under authority for homeland security, homeland defense, critical infrastructure protection, disaster/emergency assistance, and/or law enforcement. What likely matters is whether the nation is secure and defended; the individual is secure and safe; the government responds effectively, promptly, and affordably; and our civilian, representative government continues to operate to implement the Constitution and provide for the common defense.

A strategic review of national security policy and delivery of homeland security and defense services could promote integrated critical infrastructure protection, a defined national security goal. A strategic review, followed by statutory authorization, could take critical infrastructure protection beyond the stage of assess, study, inform, and report to a new stage of systematically and predictably implementing reasonable and necessary protective measures. These protective measures may include how to handle owners who do not adequately protect their

[94] *US Code* 10 (2017), §§251-255, to suppress insurrections and rebellions and to enforce federal authority and federal and state laws; §§271-284, military support for civilian law enforcement agencies, including with WMD and bombings of public places, and Title 42 disaster/emergency assistance; and other lesser-known statutory authorizations detailed in US CRS, *The Posse Comitatus Act and Related Matters*, 30 (for example, to protect Yellowstone National Park upon request by the Secretary of the Interior).

critical infrastructure and how the DHS and the DOD will work together, especially in a crisis where it may be necessary to deploy American military forces on American soil to defend it, to restore order, to enforce federal authority, to enforce federal or state law, or a combination thereof.

Appendix 1
Organization Chart for the DHS

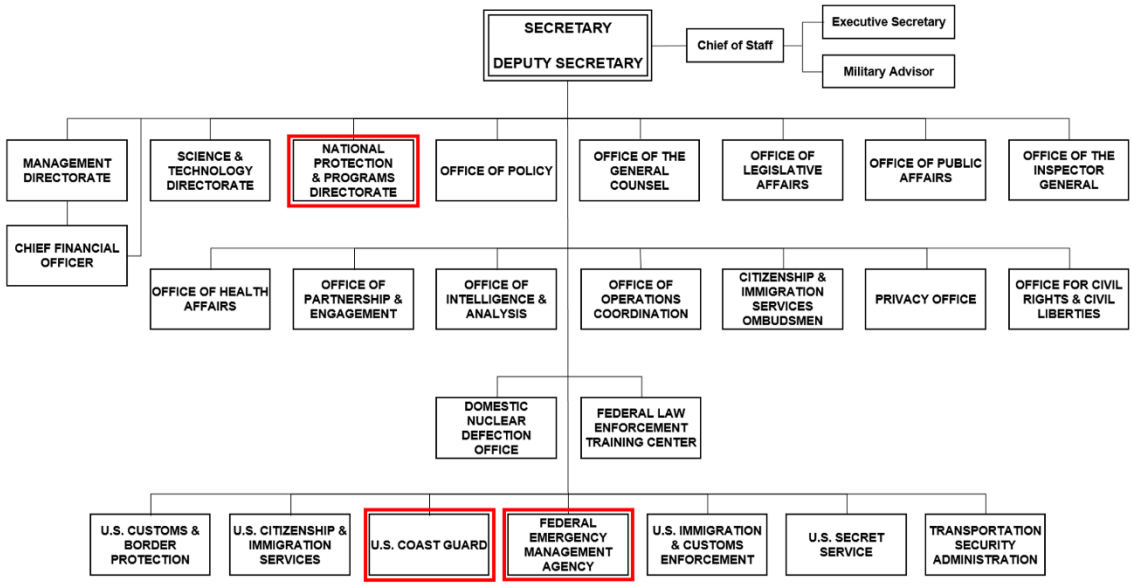

Figure 3. Organization Chart for the DHS showing the NPPD, FEMA, and USCG. Author created from US DHS, “Organization Chart,” DHS, last modified February 1, 2017, 1, accessed March 25, 2017, https://www.dhs.gov/organizational-chart.

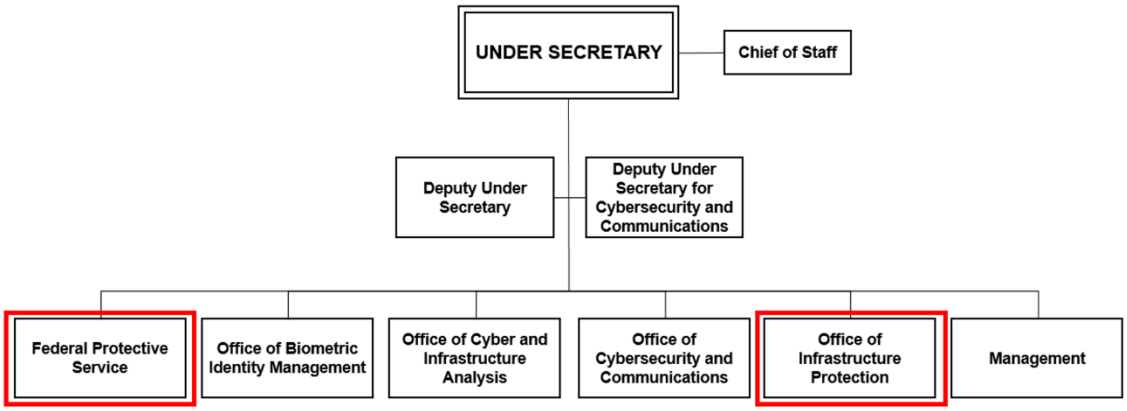

Figure 4. Organization Chart of the DHS showing NPPD's FPS and OIP. Author created from US DHS, “Organizational Chart,” 21.

Bibliography

Banks, William C., and Stephen Dycus. *Soldiers on the Home Front: The Domestic Role of the American Military*. Cambridge, MA: Harvard University Press, 2016.

Bellavita, Christopher. "85% of What You Know about Homeland Security is Probably Wrong." *Homeland Security Watch*, March 16, 2009. Accessed April 2, 2017. http://www.hlswatch.com/2009/03/16/85-percent-is-wrong/.

———. "Changing Homeland Security: What is Homeland Security?" *Homeland Security Affairs* 4 (June 2008): article 1. Accessed April 4, 2017. https://www.hsaj.org/articles/118.

Bontea, Sirius. "America's Achilles Heel: Defense Against High-Altitude Electromagnetic Pulse: Policy v. Practice." Master's thesis, US Army Command and General Staff College, 2014. Accessed March 5, 2017. http://www.dtic.mil/docs/citations/ADA613532.

Brill, Steven. "Is America Any Safer? 15 Years after 9/11." *The Atlantic*, September 2016. Accessed April 4, 2017. http://www.theatlantic.com/magazine/archive/2016/09/are-we-any-safer/492761/.

California Public Utilities Commission. *Regulation of Physical Security for the Electric Distribution System*, by Ben Brinkman, Connie Chen, Arthur O'Donnell, and Chris Parkes. February 2015. Accessed March 22, 2017. https://pdfs.semanticscholar.org/e11b/21010c0fa8e68d0958496bc3564c50524c63.pdf.

Center for the Study of the Presidency and Congress (CSPC). *Securing the U.S. Electrical Grid: Understanding the Threats to the Most Critical of Critical Infrastructure, While Securing a Changing Grid*, by Thomas F. McLarty III and Thomas J. Ridge (Washington, DC: CSPC, October 2014). Accessed January 5, 2017. https://www.thepresidency.org/sites/default/files/Final%20Grid%20Report_0.pdf.

Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures*. April 2008. Accessed January 29, 2017. http://www.empcommission.org/docs/A2473-EMP_Commission-7MB.pdf.

Friedman, Barry. "We Spend $100 Billion on Policing. We Have No Idea What Works. Police Are More Likely to Adopt New Technology Because Another Department Has It Than Because of Reasoned Cost-Benefit Analysis." *The Washington Post*, March 10, 2017. Accessed March 12, 2017. https://www.washingtonpost.com/posteverything/wp/2017/03/10/we-spend-100-billion-on-policing-we-have-no-idea-what-works/?hpid=hp_no-name_opinion-card-b%3Ahomepage%2Fstory&utm_term=.e3f11d7fbd8c.

Geiger, Deborah L. "*Posse Comitatus*, the Army, and Homeland Security: What is the Proper Balance?" Strategy Research Project, US Army War College, 2006. Accessed April 2, 2017. https://www.hsdl.org/?view&did=469535.

Grossman, Elaine M. "Former JAG: Military Aid in D.C. Sniper Pursuit May Have Broken Law." *Inside the Pentagon*, Inside Washington Publishers, November 14, 2002. Accessed April 4, 2017. https://fas.org/sgp/news/2002/11/itp111402.html.

Hayes, James K., and Charles K. Ebinger. “The Private Sector and the Role of Risk and Responsibility in Securing the Nation's Infrastructure.” *Journal of Homeland Security and Emergency Management* 18, no. 1 (March 2011): 1-25. Accessed April 2, 2017. https://www.brookings.edu/wp-content/uploads/2016/06/04_critical_infrastructure_ebinger.pdf.

Heaven, Douglas. “The Uncertain Future of Democracy.” *BBC*, March 30, 2017. Accessed March 30, 2017. http://www.bbc.com/future/story/20170330-the-uncertain-future-of-democracy.

ICF International. *Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats*. Report Prepared for US and Canadian Governments, June 2016. Accessed March 22, 2017. https://energy.gov/epsa/downloads/electric-grid-security-and-resilience-establishing-baseline-adversarial-threats.

Matthews, Matt. *The Posse Comitatus Act and the United States Army: A Historical Perspective*. Fort Leavenworth, KS: Combat Studies Institute Press, 2006.

National Archives. “The Constitution of the United States: A Transcript.” Accessed March 21, 2017. https://www.archives.gov/founding-docs/constitution-transcript.

National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling. *Deepwater: The Gulf Oil Disaster and the Future of Offshore Drilling, Report to the President*. January 11, 2011. Accessed April 2, 2017. https://www.gpo.gov/fdsys/pkg/GPO-OILCOMMISSION/content-detail.html.

Pfeffer, Robert. “Electromagnetic Threats to the National Power Grid.” *Army Chemical Review* (Winter 2010): 5-9. Accessed January 7, 2017. http://www.wood.army.mil/chmdsd/images/pdfs/Winter%202010/pfeffer.pdf.

Philpott, Don. *Understanding the Department of Homeland Security: The Cabinet Series*. New York, NY: Bernan Press, 2015.

Strategic Foresight Initiative. *Critical Infrastructure: Long-term Trends and Drivers and Their Implications for Emergency Management*. Research Report for FEMA. June 2011. Accessed April 2, 2017. https://www.fema.gov/pdf/about/programs/oppa/critical_infrastructure_paper.pdf.

Sun, Lisa Grow. “Disaster Mythology and the Law.” *Cornell Law Review* 96, no. 5 (July 2011): 1131-1207.

Tatum, Sophie, and Pamela Brown. “First on CNN: Report Finds National Security Agencies at Risk in Foreign-Owned Buildings.” *CNN*, January 30, 2017. Accessed February 1, 2017. http://www.cnn.com/2017/01/30/politics/gao-report-foreign-ownership/.

The White House, *The Federal Response to Hurricane Katrina: Lessons Learned*, by Frances Fragos Townsend. February 23, 2006. Accessed January 15, 2017. https://www.hsdl.org/?view&did=460536.

Thomson Reuters. *Guide to Homeland Security*. Eagan, MN: Thomson Reuters, 2016.

US Chemical Safety and Hazard Investigation Board. *Investigation Report: West Fertilizer Company Fire and Explosion (15 Fatalities, More than 260 Injured), West, TX April 17, 2013, Final Report 2013-02-I-TX*, January 2016. Accessed March, 5, 2017. http://www.csb.gov/west-fertilizer-explosion-and-fire-/.

US Coast Guard. "Authorities." US Coast Guard. [No date or last modified date listed on website]. Accessed March 23, 2017. http://www.overview.uscg.mil/Authorities/.

US Congress. House. Office of the Law Revision Counsel. *US Code* (2017). Accessed March 21-25, 2017, http://uscode.house.gov/browse.xhtml.

US Congress. House. Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina. A Failure of Initiative: Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina. 109th Cong., 2d sess., 2006, HR Rep. 109-377.

US Congressional Research Service. *Blackout! Are We Prepared to Manage the Aftermath of a Cyber-Attack or Other Failure of the Electrical Grid?* Written Testimony Before US Congress, by Richard Campbell. April 2016. Quoted in US Congress, House of Representatives. Blackout! Are We Prepared to Manage the Aftermath of a Cyber-Attack or Other Failure of the Electrical Grid? Hearing before the Committee on Transportation and Infrastructure. 114th Cong., 2d sess., April 14, 2016, 65-71. Accessed January 16, 2017. https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg99931/pdf/CHRG-114hhrg99931.pdf.

———. *Defining Homeland Security: Analysis and Congressional Considerations*, Report to Congress, by Shawn Reese. R42462, January 8, 2013. Accessed April 2, 2017. https://fas.org/sgp/crs/homesec/R42462.pdf.

———. *Issues in Homeland Security Policy for the 113th Congress*, by William L. Painter. R42985, February 27, 2013. Accessed April 2, 2017. https://www.hsdl.org/?view&did=732600.

———. *Physical Security of the US Power Grid: High-Voltage Transformer Substations*, by Paul W. Parfomak. R43604, July 2, 2015. Accessed February 1, 2017. https://www.everycrsreport.com/files/20150702_R43604_df43c1c3c34ecca8d6730fcca7cff108dbdd4a66.pdf.

———. *The Committee on Foreign Investment in the United States (CFIUS)*, by James K. Jackson. RL33388, February 19, 2016. Accessed April 2, 2017. https://www.hsdl.org/?view&did=790777.

———. *The Posse Comitatus Act and Related Matters: The Use of the Military to Execute Civilian Law*, by Charles Doyle and Jennifer K. Elsea. R42659, August 16, 2012. Accessed February 5, 2017. https://fas.org/sgp/crs/natsec/R42659.pdf.

US Department of Defense. Department of the Army, Headquarters. *Army Doctrine Publication (ADP) 3-28, Defense Support of Civil Authorities*. July 2012, accessed March 23, 2017, http://www.apd.army.mil/epubs/DR_pubs/DR_a/pdf/web/adp3_28.pdf.

———. *Army Doctrine Reference Publication (ADRP) 3-28, Defense Support of Civil Authorities*. June 2013, accessed March 23, 2017, http://www.apd.army.mil/epubs/DR_pubs/DR_a/pdf/web/adrp3_28.pdf.

US Department of Defense. Joint Chiefs of Staff. *Joint Publication (JP) 3-27, Homeland Defense*. July 29, 2013, accessed March 23, 2017, http://www.dtic.mil/doctrine/new_pubs/jp3_27.pdf.

———. *Joint Publication (JP) 3-28, Defense Support of Civil Authorities*. July 31, 2013, accessed March 23, 2017, http://dtic.mil/doctrine/new_pubs/jp3_28.pdf.

US Department of Homeland Security. "Ammonium Nitrate Security Program." Department of Homeland Security. October 7, 2016. Accessed March 23, 2017. https://www.dhs.gov/ammonium-nitrate-security-program.

———. "Organizational Chart." Department of Homeland Security. Last modified February 1, 2017. Accessed March 25, 2017. https://www.dhs.gov/organizational-chart.

———. "Our Mission." Department of Homeland Security. Last modified May 11, 2016. Accessed April 4, 2017. https://www.dhs.gov/our-mission.

———. *The 2014 Quadrennial Homeland Security Review*. June 18, 2014. Accessed April 2, 2017. www.dhs.gov/sites/default/files/publications/qhsr/2014-QHSR.pdf.

US Department of Homeland Security. National Protection and Programs Directorate. *Statement for the Record of Assistant Secretary Caitlin Durkovich, National Protection and Programs Directorate (NPPD), and Director David Wulf, NPPD, Before the Committee on Homeland Security, US House of Representatives*. February 27, 2014. Accessed March 23, 2017. http://docs.house.gov/meetings/HM/HM08/20140227/101787/HHRG-113-HM08-Wstate-DurkovichC-20140227.pdf.

———. *Written Testimony of NPPD Office of Infrastructure Protection Assistant Secretary Caitlin Durkovich and NPPD Office of Cybersecurity and Communications Assistant Secretary Andy Ozment for a House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies Hearing Titled "Value of DHS" Vulnerability Assessments in Protecting Our Nation's Critical Infrastructure*. July 12, 2016. Accessed April 2, 2017. https://www.dhs.gov/news/2016/07/12/written-testimony-nppd-house-homeland-security-subcommittee-cybersecurity.

US Department of Homeland Security. US Coast Guard. *BP Deepwater Horizon Oil Spill: Incident Specific Preparedness Review (ISPR), Final Report*. January 2011. Accessed January 21, 2017. http://www.uscg.mil/foia/docs/DWH/BPDWH.pdf.

US Department of State, Under Secretary for Democracy and Global Affairs. "Critical Infrastructure Protection." Department of State Archive. August 2007. Accessed April 2, 2007. https://2001-2009.state.gov/g/avianflu/91243.htm.

US General Accountability Office. *Critical Infrastructure Protection: DHS Has Made Progress in Enhancing Critical Infrastructure Assessments, but Additional Improvements Are Needed: Testimony Before the Subcommittee on Cybersecurity, Infrastructure Protection,*

and Security Technologies, Committee on Homeland Security, House of Representatives, by Chris Currie. GAO-15-692T, July 12, 2016. Accessed April 2, 2017. http://docs.house.gov/meetings/HM/HM08/20160712/105169/HHRG-114-HM08-Wstate-CurrieC-20160712.pdf.

———. *Critical Infrastructure Protection: Observations on Key Factors in DHS's Implementation of Its Partnership Approach, Testimony before the Committee on Homeland Security and Governmental Affairs, US Senate*, by Stephen L. Caldwell and Gregory C. Wilshusen. GAO-14-464T, March 26, 2014. Accessed March 12, 2017. http://www.gao.gov/assets/670/661945.pdf.

———. *Federal Real Property: GSA Should Inform Tenant Agencies When Leasing High-Security Space from Foreign Owners*, by David Wise. GAO-17-195, January 2017. Accessed April 2, 2017. http://www.gao.gov/products/GAO-17-195.

US President. Presidential Policy Directive 21. "Directive on Critical Infrastructure Security and Resilience." February 12, 2013. Accessed March 21, 2017. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil; https://www.hsdl.org/?view&did=731087.

US-Canada Power System Outage Task Force. *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*. April 2004. Accessed January 16, 2017. https://energy.gov/oe/downloads/blackout-2003-final-report-august-14-2003-blackout-united-states-and-canada-causes-and.

Vladeck, Stephen I. “Emergency Power and the Militia Acts.” *Yale Law Journal* 114 (October 2004): 149-194. Accessed February 20, 2017. http://www.yalelawjournal.org/pdf/427_pa9skxwv.pdf.