Critical Infrastructure Protection

by Patricia Ladnier

Both the Department of Homeland Security (DHS) and the Department of Defense (DoD) work to secure and defend the U.S., including protecting and securing key resources and critical infrastructure (referred to 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 is insufficient to achieve these tasks. A strategic review should realign federal statutory law to allow the DHS to implement recommendations to achieve its national security goal of critical infrastructure protection.

The statutory framework to implement constitutional authority historically authorized the DoD to defend the nation and 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

Patricia Ladnier is a management and program analyst with the U.S. Department of Homeland Security. She has earned a B.A. in Political Science/History and Economics from Graceland University, a Masters of Military Art and Science from the U.S. Army Command and General Staff College's School of Advanced Military Studies, and a JD from the University of Virginia School of Law.

Protection and Program Division's (NPPD) Federal Protective Service (FPS) and Office of Infrastructure Protection (OIP), the Federal Emergency Management Agency (FEMA), and the U.S. Coast Guard (USCG).

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 in conjunction with the General Services Administration (GSA) and the Department of Transportation (DOT) for another two. 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 U.S. critical infrastructure. Multiple reports from some post-9/11 disasters and emergencies provide observations, conclusions, and recommendations about critical infrastructure protection. Key tasks for critical infrastructure protection discussed in these reports are to establish standards and enforce compliance and physically protect and secure the critical infrastructure routinely and in an emergency. These reports made many recommendations for protective measures.

...DHS regulatory authority to set standards is very limited and offers no mechanism for an integrated, strategic, regulatory framework for critical infrastructure protection.

This article focuses on these key tasks because they appear in multiple reports and illustrate basic protective measures. These key tasks are the basis for evaluating the existing federal statutory authority for the DHS and the DoD to protect critical 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 physically protect and secure critical infrastructure.

No statutory authority exists for the DoD to issue regulations to set standards for critical infrastructure protection, which is appropriate for a civilian government. The DoD's statutory authority would permit 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 its ability to protect critical infrastructure in a crisis.

As a result, 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 emergencies 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 on the public-private partnership to achieve critical infrastructure protection. Also, regulatory 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 passage of the CIPA. Multiple reports warn of gaps in critical infrastructure protection.[6] Statutory amendments could also address two other specific considerations identified in this article: repealing the statute that criminalizes *posse comitatus* and fixing the dual-command problem.

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 article surveys federal statutory authority most relevant to protecting the nation's critical infrastructure generally and as a whole and focuses on two aspects. First, the DHS entities studied (FPS, OIP, FEMA, and the USCG) are the ones concerned generally with working to protect all sectors of critical infrastructure. This article 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 interpretation through federal executive agency regulations or judicial case law. Reviewing more than the plain meaning of the statutes exceeds the scope of this article.

The challenge of critical infrastructure protection is highly relevant, not only because of terrorism, but also because of aging and decaying infrastructure 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.

The DHS has made much progress toward a safer, more resilient nation...

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 U.S. 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

Army	Air Force
"preserving the peace and security, and providing for the defense, of the United States; supporting the national policies; implementing the national objectives; and overcoming any nations responsible for aggressive acts that imperil the peace and security of the United States." 10 US Code, (2017), §3062(a).	"preserving the peace and security, and providing for the defense, of the United States; supporting the national policies; implementing the national objectives; and overcoming any nations responsible for aggressive acts that imperil the peace and security of the United States." 10 US Code, (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." 10 US Code, (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." 10 US Code, (2017), §5063.
Source: **Author, created from identified sections of the US Code (2017), Title 10 (Armed Forces).**	

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

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 U.S., culminating in consolidating the Army, Navy and Marine Corps, and Air Force into the DoD after World War II.[10] Table 1 defines these functions.

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]

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. FEMA previously was an independent federal agency focused on disaster and emergency preparedness and response and now also, according to statutory authority, is to work 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 U.S. Navy upon a Congressional declaration of war or when the President directs.[15] The USCG's mission is to protect and defend U.S. ports, inland waterways, coastline, and territorial waters. Table 2 summarizes the major relevant responsibilities of the DHS and these DHS entities.

DHS	Coast Guard
The primary missions of the Department are to "prevent terrorist attacks within the United States; reduce the vulnerability of the United States to terrorism; minimize the damage, and assist in the recovery, from terrorist attacks that do occur within the United States; 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." 6 US Code, (2017), §111(b).	""…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." "…engage in maritime air surveillance or interdiction to enforce or assist in the enforcement of the laws of the United States." "…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 [U.S.] jurisdiction." "…maintain … readiness to function as a specialized service in the Navy in time of war." 14 US Code, (2017), §2
NPPD	
FPS (and designated DHS employees)	**OIP**
"shall protect the buildings, grounds, and property that are owned, occupied or secured by the Federal Government … and the persons on the property." 40 US Code, (2017), §1315(a).	"To access, receive, and analyze law enforcement information, intelligence information, and other information to "identify and assess the nature and scope of terrorist threats to the homeland; detect and identify threats of terrorism against the United States." "To carry out comprehensive assessments of the vulnerabilities of key resources and critical infrastructure." "To integrate relevant information, analysis, and vulnerability assessments to "identify priorities for protective and support measures regarding terrorist and other threats to homeland security." "To develop a comprehensive national plan for securing the key resources and critical infrastructure of the United States." 6 US Code, (2017), §121(d).
Source: **Author, created from identified sections of the US Code (2017), Title 6 (Domestic Security) and Title 14 (Coast Guard).**	

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

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

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

> 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

CIPA	PPD-21
Function or Sector	**Sector and Federal Agency Designated as 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: Department of Energy
Quality of life	Financial services: Department of Treasury
	Food-agriculture: Departments of Agriculture and Health & Human Services
	Government facilities: DHS, GSA
	Healthcare-public health: Department of 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.**	

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

> government services, and national security of the United States; [and] (2) 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.

Public-Private Sectors as Partners to Protect Critical Infrastructure

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, as discussed below. The ownership of U.S. 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 the critical infrastructure. 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 ensuring compliance and physically protecting and securing the infrastructure.

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 federal agencies to each sector as the responsible, sector-specific agency to each. Table 3 summarizes these CIPA and PPD-21 designations:

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] Since non-federal entities and some foreign entities own much of critical infrastructure, this doubt is important.[21] As an example, buildings owned by foreign entities, including 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 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.

Lessons from some post-9/11 disasters and emergencies

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

Establishing Standards and Enforcing Compliance

Multiple reports studying specific emergencies recommend that the government establish specific standards and enforce compliance. The 2003 U.S.-Canada task force recommended that U.S. 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 Electromagnetic Pulse (EMP) commission report succinctly stated the allocation of responsibility between industry and government and why the government must set standards:

> 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 U.S.-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 to address security concerns.[28]

Having the government set standards and enforce compliance gives infrastructure owners a common, independent guide to address security concerns.

Physically Protecting and Securing Critical Infrastructure

The electric grid attacks and the aftermath of Hurricane Katrina establish the need for routine physical security. The U.S. 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.

In the aftermath of Hurricane Katrina, the collapse of law and order illustrates the need for emergency protection of critical infrastructure. The total collapse of local law enforcement led to uncontrolled violence and civil unrest. Hurricane Katrina destroyed local government capabilities and incapacitated and overwhelmed state government, leading to calls for assistance from higher jurisdictional levels. The federal government had trouble protecting and restoring critical infrastructures after Katrina. Eventually, federal forces were decisive in helping the state National Guard to restore order in New Orleans.[30]

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 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.

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 government and persons on the property; U.S. 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.

Current regulatory authority for the DHS to establish standards and enforce compliance only addresses property owned or occupied by the federal government and persons on the property...

U.S. ports, waters, and coastline

U.S. 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. 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 U.S. territorial waters when either the president declares a national emergency or the U.S. Attorney General determines that an actual or anticipated mass migration of aliens en route to the U.S. 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 U.S., 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]

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.

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) U.S. 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.

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]

U.S. 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. 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. The USCG has broad authority to routinely enforce laws related to U.S. 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 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 U.S. 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 U.S. 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. (See Table 4)

U.S. ports, waters, and coastline

The USCG's broad statutory authority to regulate for defense and law enforcement and to protect U.S. 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 and U.S. 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, 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," rather than 18 US Code §1385's "the Army or

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." 40 US Code, (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…" 40 US Code, (2017), §1315(c).
Source: **Author created. Emphasis added by underlining and by bolding/italicizing the text in (a) that is not in (c); the difference represents a gap in defined authority to protect and to regulate.**	

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

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-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]

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.

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, TX, 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]

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.

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.

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

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]

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

Another statute authorizes the president to use militia of any state to enforce U.S. 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 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 forces may be activated upon war, national emergency, national security requirements, and National Guard forces may be activated upon actual or danger of invasion or rebellion against U.S. authority and to execute U.S. 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.

...the President has authority in a natural disaster or an emergency to deploy any federal agency...

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 WMD.[62] Both statutes require the Attorney General to request DoD assistance and are limited to emergency situations. Physically protecting and securing critical infrastructure are 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 U.S. Navy either upon a Congressional declaration of war or when the president directs.[63]

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 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"; where action is "essential to meeting immediate threats to life and property"; where it is necessary to provide emergency communication systems or emergency public transportation or fire management assistance; and 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 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 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 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 previously, interpreting and applying posse comitatus limitations to the USCG presents a challenge, especially when the USCG may be transferred to the U.S. Navy where its operations may be changed to synchronize with Navy operations.[74]

Navigating the statutory authorizations, prohibitions, limitations, and exceptions related to *posse comitatus* is like a maze.

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 Figure 1 (page 20).

The governor of a state may mitigate the parallel command challenge by agreeing to appointment of a dual-status commander, as illustrated in Figure 2 (page 21). However, nothing in federal law requires the governor to agree to the 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

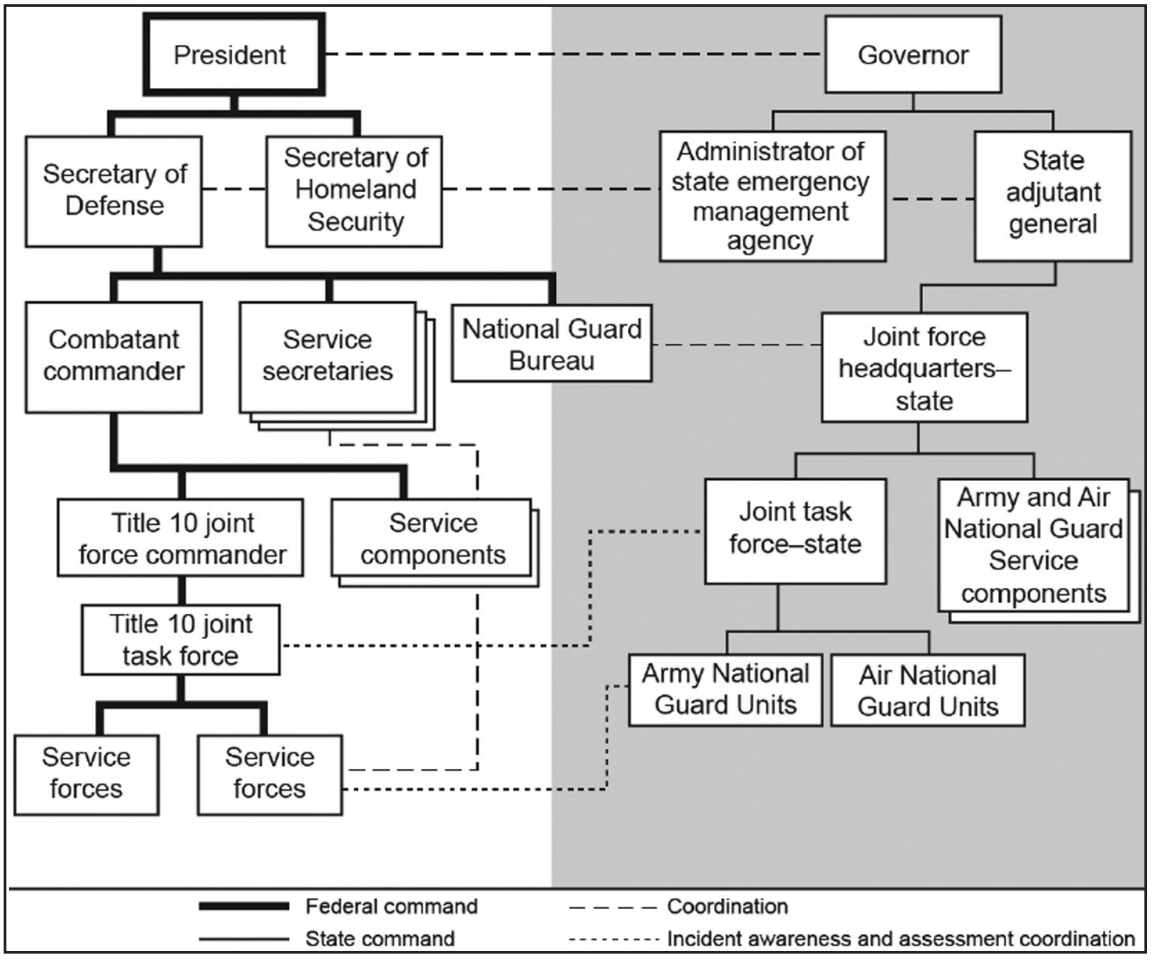

Figure 1. Dual/Parallel Command Structure with Federalized State National Guard.
Source: **U.S. DoD, Department of the Army, Headquarters, ADRP 3-28, Defense Support of Civil Authorities, p. 3-9 (Figure 3-5. Example of parallel command structure).**

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]

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

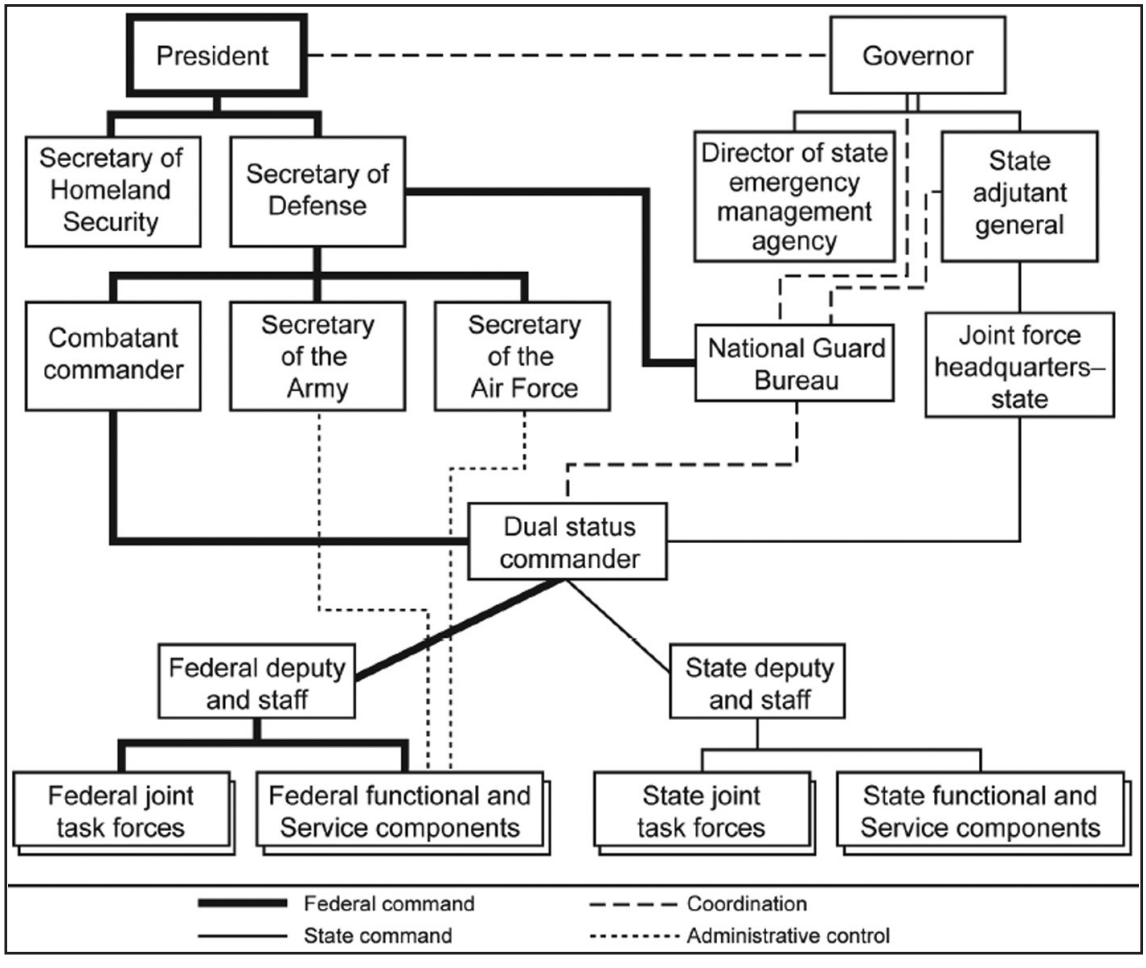

Figure 2. Dual Status Command Solution with Federalized State National Guard.
Source: **U.S. DoD, Department of the Army, Headquarters, ADRP 3-28, Defense Support of Civil Authorities, p. 3-10 (Figure 3-6. Example of dual-status command structure).**

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 the DoD's ability to perform this task as effectively as needed.

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. U.S. 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 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.

Neither [DHS or DoD] has federal statutory authority for an integrated plan or response to critical infrastructure protection.

Strategic Review for Integrated National Security and Critical Infrastructure Protection

These deficiencies and others suggested by this article present the need for a strategic review to integrate national security and critical infrastructure protection policy. The U.S. previously has moved to integrate national security policy. In 1947, Congress articulated the need for integrated, comprehensive, and strategic U.S. 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 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 U.S., 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 model—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]

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; concerned citizens; retired members of the U.S. 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.

Congress must be committed to act on reasoned recommendations to secure our nation's critical infrastructure, rather than reacting to the next crisis.

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 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 U.S. 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 that specifically authorizes 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]

- 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 U.S. military.

Conclusion

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]

When the U.S. calls forth the militia (now the National Guard) to execute the laws of the Union, the militia should be in the service of the U.S.[93] In addition, the regular U.S. military forces (non-National Guard) are authorized by statutory law to act domestically in certain 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 when he or she 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 U.S. 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 stages 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 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. ***IAJ***

NOTES

1 "Critical Infrastructures Protection Act of 2001," Public Law 107-56, 115 Stat 400, October 26, 2001, codified at 42 US Code, §5195c, <http://uscode.house.gov/browse.xhtml>, accessed on March 21, 2017.*

2 "Homeland Security Act of 2002," Public Law 107-296, 116 Stat 2135, codified at 6 US Code, 2017, §§101 et seq., <http://uscode.house.gov/browse.xhtml>, accessed on March 21, 2017.

3 ICF International, *Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats*, June 2016, pp. 88 and 91, <https://energy.gov/epsa/downloads /electric-grid-security-and-resilience-establishing-baseline-adversarial-threats>, accessed on March 22, 2017; 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*, Vol. 18, No. 1, March 2011, p. 2, <https://www.brookings.edu/wp-content/uploads/2016/06/04_critical _infrastructure_ebinger.pdf>, accessed on April 2, 2017.

4 "Critical Infrastructures Protection Act of 2001," 42 US Code §5195c(e).

5 "Homeland Security Act of 2002," 6 US Code §456; William C. Banks and Stephen Dycus, *Soldiers on the Home Front: The Domestic Role of the American Military*, Harvard University Press, Cambridge, 2016, p. 11; Shawn Reese, *Defining Homeland Security: Analysis and Congressional Considerations*, U.S. Congressional Research Service (CRS) report to Congress, Washington, DC, January 8, 2013, Summary,

<https://fas.org/sgp/crs/homesec /R42462.pdf>, accessed on April 2, 2017. This CRS report concludes that the U.S. 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."

6 Chris Currie, "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, GAO-15-692T, Washington, DC, July 12, 2016, <http://docs.house.gov/meetings/HM/HM08/20160712 /105169/HH"RG-114-HM08-Wstate-CurrieC-20160712.pdf>, accessed on April 2, 2017; Richard Campbell, *Blackout! Are We Prepared to Manage the Aftermath of a Cyber-Attack or Other Failure of the Electrical Grid?*, written testimony before U.S. Congress, U.S. Government Printing Office, Washington, DC, April 2016, quoted in hearing before the Committee on Transportation and Infrastructure, 114th Cong., 2d sess., April 14, 2016, p. 65, <https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg99931/pdf/CHRG-114hhrg99931.pdf>, accessed on January 16, 2017; Ben Brinkman, et al., *Regulation of Physical Security for the Electric Distribution System*, California Public Utilities Commission, February 2015, pp. 3, 6, and 13, <https://pdfs.semanticscholar.org/e11b /21010c0fa8e68d0958496bc3564c50524c63.pdf,> accessed on March 22, 2017; Thomas F. McLarty III and Thomas J. Ridge, *Securing the U.S. Electrical Grid: Understanding the Threats to the Most Critical of Critical Infrastructure, While Securing a Changing Grid*, Center for the Study of the Presidency and Congress (CSPC), Washington, DC, October 2014, <https://www.thepresidency.org/sites/default/files /Final%20Grid%20Report_0.pdf>, accessed on January 5, 2017.

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

8 Some thought-provoking articles relevant to issues in homeland security and defense that question the effectiveness of the status quo include: Steven Brill, "Is America Any Safer? 15 Years after 9/11," *The Atlantic*, September 2016, <http://www.theatlantic.com /magazine/archive/2016/09/are-we-any-safer/492761/>, accessed on April 4, 2017. 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, <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>, accessed on March 12, 2017. Friedman discusses the increasing cost of policing, including weapons and other systems, and questions the effectiveness of expensive new technology; Douglas Heaven, "The Uncertain Future of Democracy," BBC, March 30, 2017, http://www.bbc.com/future /story/20170330-the-uncertain-future-of-democracy>, accessed on March 30, 2017. Heaven discusses trends in democratic countries, including alarming moves in some countries toward the certainty and security offered by authoritarianism.

9 U.S. Constitution, Preamble; Article 1, Section 8; Article. 4, Section. 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, pp. 43–46;

Stephen I. Vladeck, "Emergency Power and the Militia Acts," *Yale Law Journal*, Vol. 114, 2004, pp. 149–194, <http://www.yalelawjournal.org /pdf/427_pa9skxwv.pdf,> accessed on February 20, 2017. 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. "Critical Infrastructures Protection Act of 2001," 42 US Code §5195(c)(2); "Homeland Security Act of 2002," 6 US Code §121(d). These two statutes set forth national policy related to critical infrastructure protection and the public-private partnership. Thomson Reuters, *Guide to Homeland Security*, Thomson Reuters, Eagan, MN, 2016, pp. 1–5. This source gives background on the DHS.

10 "The National Security Act of 1947," Public Law 114-328, 61 Stat 496, July 26, 1947, codified at 50 US Code §3002, Chapter 343.

11 Joint Chiefs of Staff, Joint Publication 3-27, *Homeland Defense*, U.S. Department of Defense, Washington, DC, July 29, 2013, <http://www.dtic.mil/doctrine /new_pubs/jp3_27.pdf>, accessed on March 23, 2017; Joint Chiefs of Staff, Joint Publication 3-28, *Defense Support of Civil Authorities*, U.S. Department of Defense, Washington, DC, July 2012, June 2013, July 31, 2013, <http://dtic.mil/doctrine / new_pubs/jp3_28.pdf>, accessed on March 23, 2017.

12 Joint Publication 3-27, *Homeland Defense*, p, I-1.

13 "Organizational Chart," Department of Homeland Security, last modified February 1, 2017, pp. 1 and 21, <https://www.dhs.gov/organizational-chart>, accessed on March 25, 2017; "Information Analysis and Infrastructure Protection," 6 US Code, 2017, §121 and "Definitions" 6 US Code, 2017, §311 et seq. (FEMA); "Coast Guard and Maritime Transportation Act of 2012," Public Law 112-213, 126 Stat 1540, December 20, 2012, codified at 14 US Code §3, (Coast Guard).

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

15 "Establishment of Coast Guard," 14 US Code, §1, and §3 (a) and (b).

16 "The Homeland Security Act of 2002." This act defines "American homeland" and "homeland" as "the United States" but contains no definition for homeland security. "Our Mission," DHS, <https://www.dhs.gov/our-mission," last modified May 11, 2016, accessed on April 4, 2017. "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*, Vol. 4, June 2008, <https://www.hsaj.org/articles/118>, accessed on April 4, 2017.

17 "Critical Infrastructure Protection Act of 2001," 42 US Code, 2017, §5195c(b)(3) and (c)(1) and (2).

18 "Critical Infrastructure Protection Act of 2001," 42 US Code, 2017, §5195c(e).

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

20 ICF International, pp. 88 and 91. This report was prepared for the U.S. and Canadian governments. It demonstrates that most utilities are investor-owned, and that it is difficult to achieve results across the grid. Brinkman et al., pp. 3, 6, and 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, U.S. Government Printing Office, Washington, DC, January 11, 2011, pp. 118–127,

<https://www.gpo.gov/fdsys/pkg/GPO-OILCOMMISSION/content-detail.html>, accessed on April 2, 2017. 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, <https://www.fema.gov/pdf/about/programs/oppa/critical_infrastructure_paper.pdf>, accessed on April 2, 2017. This research and report was prepared for FEMA. U.S. Department of State, Under Secretary for Democracy and Global Affairs, "Critical Infrastructure Protection," August 2007, <https://2001-2009.state.gov/g/avianflu /91243.htm>, accessed on April 2, 2007. This article discusses how critical infrastructure is interconnected even outside the U.S., including in Canada and Mexico. Christopher Bellavita, "85% of What You Know about Homeland Security is Probably Wrong," *Homeland Security Watch*, March 16, 2009, <http://www.hlswatch.com/2009/03/16/85-percent-is-wrong/>, accessed on April 2, 2017. Bellavita critiques the commonly-used 85 percent figure used to describe private-sector ownership of critical infrastructure. U.S. Campbell (see Note 6 above) 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 David Wise, "Federal Real Property: GSA Should Inform Tenant Agencies When Leasing High-Security Space from Foreign Owners," GAO-17-195, Washington, DC, January 2017, pp. 2, 13, and 20, <http://www.gao.gov/products/GAO-17-195>, accessed on April 2, 2017; Sophie Tatum and Pamela Brown, "First on CNN: Report Finds National Security Agencies at Risk in Foreign-Owned Buildings," CNN, January 30, 2017, <http://www.cnn.com/2017/01/30/politics/gao-report-foreign-ownership/>, accessed on February 1, 2017; James K. Jackson, *The Committee on Foreign Investment in the United States (CFIUS)*, U.S. CRS, RL33388, Washington, DC, February 19, 2016, pp. 30–31, <https://www.hsdl.org/?view&did=790777>, accessed on April 2, 2017.

23 William L. Painter, *Issues in Homeland Security Policy for the 113th Congress*, U.S. CRS R42985, Washington, DC, February 27, 2013, p. 3, <https://www.hsdl.org /?view&did=732600>, accessed on April 2, 2017. 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."

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, p. 139, <https://energy.gov/oe/downloads/blackout-2003-final-report-august-14-2003-blackout-united-states-and-canada-causes-and>, accessed on January 16, 2017.

25 ICF International, pp. 88 and 91; Brinkman et al.; GAO-15-692T, pp. 6–7, 10, and 16–17; National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, pp. 118–127.

26 National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, pp. 118–127.

27 Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, "Critical National Infrastructures," report, April 2008, p. 53, <http://www.empcommission.org/docs/A2473-EMP_Commission-7MB.pdf>, accessed on January 29, 2017.

28 US-Canada Power System Outage Task Force, p. 21; National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, pp. 126–127 and 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, pp. 53–54, 57, 59–60, 80–81, 104, 155, 157, and173. 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 requiring gasoline and diesel fuel distribution facilities to have on-site power generation in the event of electrical grid failure, testing and installing electrical equipment, requiring incorporation of new technology in telecommunications infrastructure, and improving the hardening of oil and gas control systems to avoid damage from EMP effects.

29 Paul W. Parfomak, *Physical Security of the US Power Grid: High-Voltage Transformer Substations*, U.S. CRS R43604, Washington, DC, July 2, 2015, pp. 2, 30, and 32, <https://www.everycrsreport.com/files/20150702_R43604 _df43c1c3c34ecca8d6730fcca7cff108dbdd4a66.pdf>, accessed on February 1, 2017; Brinkman et al., pp. iii-iv, 3, 6, 13, and 29; ICF International, pp. 14–16, 88, and 91.

30 Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina, "A Failure of Initiative," final report, 109th Cong., 2d sess., 2006, HR Rep. 109-377, pp. 1 and 3, <https://www.gpo.gov/fdsys/pkg/CRPT-109hrpt377/pdf/CRPT-109hrpt377.pdf>, accessed January on 15, 2017; The White House, *The Federal Response to Hurricane Katrina: Lessons Learned*, Washington, DC, February 23, 2006, pp. 40–43 and 61, <https://www.hsdl.org/?view&did=460536>, accessed on January 15, 2017.

31 6 US Code §457 mandates that: "Except 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 article, 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, 128 Stat 2898, codified at 6 US Code §621 et seq. and "Consolidated Appropriations Act," 2008, Subtitle J, Secure Handling of Ammonium Nitrate, Public Law 110-161 (Title V, Section 563), 121 Stat 2083, codified at 6 US Code §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.

32 "Coast Guard Authorization Act of 2010," Public Law 111-281, (Title VIII, §820[a]), 124 Stat 3001, codified at 46 US Code §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]. 14 US Code §100 authorizes the USCG to enforce 46 US Code, Chapter 551, Coastwise Trade Laws. For an overview, see USCG, "Authorities," <http://www.overview.uscg.mil/Authorities/>, accessed on March 23, 2017.

33 50 US Code, (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," Public Law 104-208, Div. C, Title VI, §649, 110 Stat 3009-711 and "Coast Guard and Maritime Transportation Act of 2004," Public Law 108-293, Title II, §223, 118 Stat 1040.

34 14 US Code §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 [U.S.] jurisdiction." 14 US Code §2(1). If the Federal Aviation Administration (FAA) or the U.S. Air Force (USAF) do not regulate low-flying drones over U.S. 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, 124 Stat 2970, codified at 46 US Code §1 and §3306.

36 USCG, "Authorities," <http:www.overview.uscg.mil/Authorities>, accessed on March 23, 2017.

37 6 US Code §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 6 US Code §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. DHS, "Ammonium Nitrate Security Program," October 7, 2016, <https://www.dhs.gov/ammonium-nitrate-security-program>, accessed on March 23, 2017.

39 "Homeland Security Act of 2002," Public Law 107-296, Title XVII, §1706(b)(1), 116 Stat 2317, codified at 40 US Code §1315(b)(1).

40 14 US Code §141.

41 14 US Code §2(1), (2), law enforcement, maritime aerial surveillance; §89, law enforcement; §95(a)(1), (2) and §99, carrying firearms and making arrests; 14 US Code §100, authority to enforce chapter 551 of title 46, coastwise trade laws (shipping and transportation); 14 US Code §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 50 US Code §191.

43 14 US Code §2(7), §1 and §3.

44 Matt Matthews, *The Posse Comitatus Act and the United States Army: A Historical Perspective*, Combat Studies Institute Press, Fort Leavenworth, KS, 2006, pp. 1–46; Banks and Dycus, pp. 92–93 and 105–112; Charles Doyle and Jennifer K. Elsea, *The Posse Comitatus Act and Related Matters: The Use of the Military to Execute Civilian Law*, CRS R42659, Washington, DC, August 16, 2012, pp.19–20, <https://fas.org/sgp/crs/natsec/R42659.pdf>, accessed on February 5, 2017.

45 "National Defense Authorization Act for Fiscal Year 2017," Public Law 114-328, Div. A., Title XII, §1241(a)(2), 130 Stat 2497, codified at 10 US Code §275 (renumbered from 50 US Code §375).

46 Doyle and Elsea, p. 4. The USCG is not mentioned in the *posse comitatus* prohibitions, and "as a practical matter, however, the USCG is statutorily authorized to perform law enforcement functions." Banks and Dycus, p. 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 U.S. Navy.

47 6 US Code §466.

48 14 US Code §141.

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

50 "Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014," Public Law 113-254, 128 Stat 2919, set forth in note following 6 US Code §621.

51 Painter, p. 22.

52 Caitlin Durkovich and David Wulf, statement for the record before the Committee on Homeland

Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, U.S. House of Representatives Washington, DC, February 27, 2014, <http://docs.house.gov/meetings/HM/HM08/20140227/101787 /HHRG-113-HM08-Wstate-DurkovichC-20140227.pdf>, accessed on March 23, 2017.

53 U.S. Chemical Safety and Hazard Investigation Board, "West Fertilizer Company Fire and Explosion (15 Fatalities, more than 260 Injured)," final investigation report, Washington, DC, January 2016, pp. 55 and175, <http://www.csb.gov/west-fertilizer-explosion-and-fire-/>, accessed on March 5, 2017. The fertilizer, blending, retail, 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. 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 Currie, p. 10.

55 6 US Code §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.

56 "Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005," Public Law 108-375, Div. A, Title V, §512(a)(1), 118 Stat 1811, codified at 32 US Code §§901–908.

57 10 US Code §251.

58 10 US Code §252.

59 10 US Code §253.

60 10 US Code §§10102 and 12406.

61 10 US Code §283(a) and 18 US Code §2332f.

62 10 US Code §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." 10 US Code §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 title18 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." 18 US Code §175, biological weapons; 18 US Code §229, chemical weapons; 18 US Code §2332a, weapon of mass destruction.

63 14 US Code §1 and §3.

64 "Robert T. Stafford Disaster Relief and Emergency Assistance Act," Public Law 100-707, 102 Stat 4696, codified at 42 US Code §5170(a), (b), major disaster; §5191(a), (c), emergency assistance. Both statutes also permit a request by an Indian tribal chief executive. 42 US Code §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 42 US Code §5170a, major disaster assistance; §5191(a), emergency assistance.

66 42 US Code §5170(a)(5) and §5191(b)(5), "where necessary to save lives, prevent human suffering, or mitigate severe damage." 42 US Code §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. 42 US Code §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 32 US Code §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.

68 32 US Code §904(b). The statute limits this duty to 180 days. The time may be extended once for 90 days "to meet extraordinary circumstances."

69 32 US Code §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, U.S. Army Command and General Staff College, 2014, <http://www.dtic.mil/docs /citations/ADA613532>, accessed on March 5, 2017.

71 10 US Code §274, §275, §282, and §283.

72 10 US Code §275 specifies "Army, Navy, Air Force, or Marine Corps" and 18 US Code §1385 specifies "Army or Air Force."

73 Doyle and Elsea, p. 30. This report lists twenty-two statutory exceptions to the *Posse Comitatus* Act. This list does not include, however, 10 US Code §§271–284, some of which contain additional exceptions to the posse comitatus prohibition. Banks and Dycus, pp. 103 and 193–195.

74 14 US Code §3(b).

75 10 US Code §5170(a)(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 DHS, USCG, "Incident Specific Preparedness Review (ISPR) Deepwater Horizon Oil *Spill,"* final report, Washington, DC, January 2011, p. 9, <http://www.uscg.mil/foia/docs /DWH/BPDWH.pdf>, accessed on January 21, 2017. 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.

77 "The National Security Act of 1947," Public Law 114-328, Chapter 343, §2, 61 Stat 496, subsequently amended and codified at 50 US Code §3002.

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

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

80 6 US Code §121(d) and §124l.

81 6 US Code §456. Reese, 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, pp. 11, 265, and 274–275. 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." Painter, pp. 1 and 3. This 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."

82 6 US Code §§111(b)(1), 121(d).

83 Hayes and Ebinger, pp. 1–2 and 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, p. 88.

84 6 US Code §124, national asset database and prioritized list. Stephen L. Caldwell and Gregory C. Wilshusen, "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, U.S. Senate, GAO-14-464T, Washington, DC, March 26, 2014, p. 6, <http://www.gao.gov/assets/670/661945.pdf>, accessed on March 12, 2017. 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 this article, in addition to the DHS, USCG, "Incident Specific Preparedness Review (ISPR) Deepwater Horizon Oil Spill," final report, p. 9.

86 Banks and Dycus, pp. 91–92 and 105–106.

87 The White House, pp. 54–55.

88 Banks and Dycus, pp. 107–108; Doyle and Elsea, p. 1.

89 Banks and Dycus, p. 275. The way the *posse comitatus* doctrine has evolved in the U.S. should 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, U.S. Army War College, 2006, <https://www.hsdl.org/?view&did=469535>, accessed on April 2, 2017. Geiger 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 18 US Code §1385, previously was in Title 10 but was moved to Title 18 (Crimes) in 1956. 70A Stat 626.

91 10 US Code §275 (DoD); 6 US Code §466 (DHS); Doyle and Elsea, p. 30; Banks and Dycus, pp. 103 and 193–195; see Table 5.

92 U.S. Constitution, Preamble and Art. 1, Sec 8.

93 10 US Code §12406. The National Guard may be activated to federal service where invasion or danger of invasion; rebellion or danger of rebellion against U.S. authority; or "the President is unable with the regular forces to execute the laws of the United States." Doyle and Elsea, p. 30. This report lists this statute as a statutory exception to the Posse Comitatus Act.

94 10 US Code §§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 Doyle and Elsea, p. 30 (for example, to protect Yellowstone National Park upon request by the Secretary of the Interior).

* All references to the US Code 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.