An Analysis of the Primary Authorities Supporting and Governing the Efforts of the Department of Homeland Security to Secure the Cyberspace of the United States

Final Report

24 May 2011

HOMELAND SECURITY
STUDIES AND ANALYSIS INSTITUTE

An FFRDC operated by Analytic Services Inc. on behalf of DHS

2900 South Quincy Street • Suite 800
Arlington, VA 22206-2233

Prepared for the
Department of Homeland Security
Science and Technology Directorate

HOMELAND SECURITY STUDIES AND ANALYSIS INSTITUTE

The Homeland Security Act of 2002 (Section 305 of PL 107-296, as codified in 6 U.S.C. 185), herein referred to as the "Act," authorizes the Secretary of the Department of Homeland Security (DHS), acting through the Under Secretary for Science and Technology, to establish one or more federally funded research and development centers (FFRDCs) to provide independent analysis of homeland security issues. Analytic Services Inc. operates the HOMELAND SECURITY STUDIES AND ANALYSIS INSTITUTE as a FFRDC for DHS under contract HSHQDC-09-D-00003.

The Institute provides the government with the necessary expertise to conduct: cross-cutting mission analysis, strategic studies and assessments, development of models that baseline current capabilities, development of simulations and technical evaluations to evaluate mission trade-offs, creation and evolution of high-level operational and system concepts, development of top-level system and operational requirements and performance metrics, operational analysis across the homeland security enterprise, and analytic support for operational testing evaluation in tandem with the government's acquisition process. The Institute also works with and supports other federal, state, local, tribal, public and private sector organizations that make up the homeland security enterprise.

The Institute's research is undertaken by mutual consent with DHS and is organized as a set of discrete tasks. This report presents the results of research and analysis conducted under

Task 10-01.04.02
A Strategic Look at Cyber Security Policy

The results presented in this report do not necessarily reflect official DHS opinion or policy.

HOMELAND SECURITY STUDIES & ANALYSIS INSTITUTE
An FFRDC operated by Analytic Services Inc. on behalf of DHS

Task Lead
Matthew H. Fleming, PhD
Fellow

Eric Goldstein
Senior Associate Analyst

Robert Tuohy
Vice President and Deputy Director, Operations

AN ANALYSIS OF THE PRIMARY AUTHORITIES SUPPORTING AND GOVERNING THE EFFORTS OF THE DEPARTMENT OF HOMELAND SECURITY TO SECURE THE CYBERSPACE OF THE UNITED STATES

FINAL REPORT

24 May 2011

Prepared for
Department of Homeland Security
Science and Technology Directorate

ACKNOWLEDGEMENTS

The authors wish to thank a number of anonymous referees, as well as James A. Lewis, Director and Senior Fellow, Technology and Public Policy Program, Center for Strategic and International Studies (CSIS); Adriane Lapointe, Visiting Fellow, Technology and Public Policy Program, CSIS; Neal A. Pollard, Principal, PRTM Management Consultants; and Blaise Misztal, Associate Director of Foreign Policy and Director, Cyber Security Task Force, Bipartisan Policy Center.

For information about this publication or other HSI research, contact:

HOMELAND SECURITY STUDIES AND ANALYSIS INSTITUTE
Analytic Services Incorporated
2900 S. Quincy Street
Arlington, VA 22206
Tel (703) 416-3550
Fax (703) 416-3530
www.homelandsecurity.org

RP10-01.04.02-01

TABLE OF CONTENTS

(This page intentionally blank)

EXECUTIVE SUMMARY

The Department of Homeland Security (DHS) has a central role to play in the cybersecurity of the United States (U.S.). This role is summarized in the department's own 2010 *Bottom-Up Review Report*, which notes that "by statute and Presidential directive, DHS has the lead for the Federal government to secure civilian government computer systems, works with industry to defend privately-owned and operated critical infrastructure, and works with State, local, tribal and territorial governments to secure their information systems" (DHS 2010a). However, authorities governing and supporting this central role appear to lack sufficient clarity. As a result, it remains difficult to judge their adequacy—and, more importantly, the fundamental nature and extent of the department's role in securing U.S. cyberspace.

In an attempt to provide clarity to the national cybersecurity community, staff from the Homeland Security Studies and Analysis Institute (HSI) conducted research to determine: what are the primary authorities supporting/governing DHS efforts to secure U.S. cyberspace (and what do the authorities say); and what ambiguities, conflicts, and gaps appear to exist in these authorities (and what are their implications for the DHS mission). This paper presents the findings of the research. It is designed to serve as a foundational document for use by DHS and its partners in the U.S. government (USG) and broader homeland security enterprise.

Overall, the research suggests that existing DHS-related authorities may not be fully sufficient for DHS to: require or incentivize the protection of critical systems and information; gather (i.e., collect) information to be shared; define clearly when DHS may intervene during a cyber incident; support actions necessary to manage and coordinate cyber incident response, including for the most serious of incidents; and delineate the responsibilities of DHS and DoD for the most serious of incidents.

(This page intentionally blank)

I. INTRODUCTION

The Department of Homeland Security (DHS) has a central role to play in the cybersecurity of the United States (U.S.). This role is summarized in the department's own 2010 *Bottom-Up Review Report* (BUR), which notes that "by statute and Presidential directive, DHS has the lead for the Federal government to secure civilian government computer systems, works with industry to defend privately-owned and operated critical infrastructure, and works with State, local, tribal and territorial governments [SLTTGs] to secure their information systems" (DHS 2010a).

The exact nature and implications of the legal authorities that allow DHS to carry out its cybersecurity mission, however, remain unclear. For example, while DHS "has the lead" for the federal government to secure civilian government computer systems, it appears to have no formal enforcement authority to compel federal government departments and agencies to apply recommended cybersecurity mitigations (Skinner 2010). Further, as noted above, DHS "works with" the private sector and SLTTGs to promote the security of their critical information systems. But this can imply a variety of potentially voluntary or involuntary activities (like threat and vulnerability information sharing or incident reporting)—many of which have not been defined with sufficient precision.

A lack of clarity on the nature and implications of authorities presents conditions for potentially dangerous mission failure. Here the lessons of incidents like Hurricane Katrina—cyber-related or not—are significant. Chief among these might be that a lack of clear roles and responsibilities, which flow from authorities, can result in ineffective command and control—and thus poor incident response, with tragic consequences (White House 2006).

Accordingly, in an attempt to provide clarity to the national cybersecurity community, staff from the Homeland Security Studies and Analysis Institute (HSI) conducted research to determine: what are the primary authorities supporting/governing DHS efforts to secure U.S. cyberspace (and what do the authorities say); and what ambiguities, conflicts, and gaps appear to exist in these authorities (and what are their implications for the DHS mission). This paper presents the findings of the research. It is designed to serve as a foundational document for use by DHS and its partners in the U.S. government (USG) and broader homeland security enterprise.

The paper is structured as follows: after this introduction, a background chapter defines cyberspace, cybersecurity, the cybersecurity landscape, authorities, the motivation for the research, and the research questions, methodology, and scope; a subsequent chapter presents the primary DHS-related authorities on cybersecurity; a discussion chapter examines the implications of ambiguities, conflicts, and gaps in DHS-related authorities on cybersecurity; and a conclusion summarizes and closes with thoughts for future research.

II. BACKGROUND

This chapter serves to define cyberspace, cybersecurity, and the cybersecurity landscape; provide a general overview of authorities; and present the motivation for the research and the research questions, methodology, and scope.

A. Cyberspace, Cybersecurity, and the Cybersecurity Landscape

Cyberspace refers to "the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people" (White House 2009a, citing National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (NSPD-54/HSPD-23)).[1]

The United States relies on cyberspace in nearly all aspects of life. In sum, "the globally-interconnected digital information and communications infrastructure known as 'cyberspace' underpins almost every facet of modern society and provides critical support for the U.S. economy, civil infrastructure, public safety, and national security" (White House 2009a). Indeed, cyberspace underpins the bulk of U.S. critical infrastructure/key resources (CIKR), including banking and finance, energy, communications, transportation (such as air traffic control), and the like.

Through cyberspace, malicious actors, accidents, and natural hazards can cause kinetic and nonkinetic effects such as the physical failure of the power grid, the manipulation of financial data, or the loss of intellectual property.[2] These effects result in physical, economic, psychological, etc. costs to the nation, including (potentially) loss of life.[3] Because of the U.S. reliance on cyberspace, these costs may be very significant.[4]

---

[1] For glossary definitions on cyberspace and also information assurance, see Joint Chiefs of Staff (2010) and Committee on National Security Systems (2010). Note, however, that some uncertainty exists in the cybersecurity community on the underlying meanings of terms (and their associated implications), including phrases like cyberwar and cyberattack.

[2] For useful background information on cybersecurity and the cyber threat, see Masters (2011). To date, perhaps the most infamous cyber-physical event has involved the "Stuxnet" worm, which appears to have targeted Iranian uranium enrichment centrifuges. For a journalistic account of Stuxnet, see Gross (2011); for a technical overview, see Falliere et al. (2011).

[3] Malicious actors include state/nonstate actors, criminals, "hacktivists," etc.; accidents include software/hardware failures and human error; and natural hazards include earthquakes, hurricanes, floods, tornadoes. Kinetic and/or nonkinetic effects are caused when malicious actors copy, manipulate, or deny timely access to or delete data—including intellectual property, personally identifiable information, data that facilitate services or relate to industrial control systems—or when these outcomes are caused by accidents or natural hazards.

[4] At present, no agreed methods for measuring the costs of cyber incidents exist. Various estimates prevail in the literature, measuring various elements of the cybersecurity problem

Cybersecurity activities seek to minimize these costs. Cybersecurity activities include "the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure" (White House, 2009a).[5]

While cybersecurity activities are carried out by virtually all users of cyberspace—even private citizens have at least a nominal role to play—primary entities in the U.S. cybersecurity enterprise include federal government departments and agencies (e.g., the Executive Office of the President, DHS, Departments of Defense, Justice, State, Commerce, Treasury, Energy, and the intelligence community (IC)); SLTTGs (including the Multi-State Information Sharing and Analysis Center (MS-ISAC)); and private-sector partners (especially owner/operators of CIKR assets and CIKR sector ISACs, as well as the companies that design and produce the components of cyberspace).[6]

B. Understanding Authorities

This paper explores the legal "authorities" that support and govern DHS efforts to secure U.S. cyberspace. Authorities provide DHS (like other federal departments and agencies) its ability to act. Broadly, authorities are categorized as "primary" or "secondary." Primary authorities carry force of law and generally are binding; they include the U.S. Constitution, legislation, executive orders (EOs, including presidential directives (PDs)), administrative regulations, court opinions (case law), treaties, etc.[7] Secondary authorities serve to summarize or interpret the meanings and implications of primary authorities and

(some doing so more credibly than others). For example, a 2004 Congressional Research Service report estimated that the annual cost of malicious intrusions was up to $226 billion at that time (Cashell 2004). A 2010 white paper by the Internet Security Alliance (ISA) estimated that the cost to the U.S. of the theft of intellectual property was $1 trillion. Some cyber incidents, not least those affecting CIKR assets, may have more systemic second- and third-order effects, and thus incur potentially significant costs across sectors (see NIAC 2007).

[5] Note that the quote, as it exists in White House (2009a), serves to define "cybersecurity policy"; it is used here to set forth a listing of cybersecurity activities. For a catalog of cybersecurity activities at the organizational level, see Special Publication 800-53 of the National Institute of Standards and Technology (NIST 2010) and also the "Twenty Critical Security Controls for Effective Cyber Defense" assembled by the SANS Institute (SANS 2009).

[6] For a comprehensive list of relevant cybersecurity entities in the U.S.—and their incident response roles—see the interim National Cyber Incident Response Plan (NCIRP; DHS 2010b). Perhaps not surprisingly, the U.S. cybersecurity enterprise mirrors the homeland security enterprise, which is defined by the Quadrennial Homeland Security Review (QHSR) as "the federal, state, local, tribal, territorial, nongovernmental, and private-sector entities, as well as individuals, families, and communities who share a common national interest in the safety and security of America and the American population" (DHS 2010d).

[7] While EOs may be considered binding within the executive branch, they generally do not include enforcement mechanisms or penalties for non-compliance. As a result, implementation may be viewed as somewhat discretionary at the department or agency level.

are nonbinding (but persuasive); they include executive agency plans and reviews, legal texts, treatises, journal articles (e.g., law review articles), etc.[8] The present research focuses on primary authorities (see "Research Questions, Methodology, and Scope," p. 8).

Authorities of the federal government are inherently governed by the U.S. Constitution, through the responsibilities of the legislative branch outlined in Article I, the executive branch in Article II, and the judicial branch in Article III. Under Article I, Congress is empowered to enact legislation governing the affairs of the United States in specific areas, particularly, in the context of the present paper, to regulate interstate commerce, make rules for the government, and make laws necessary and proper for executing all of the powers vested in Congress by the U.S. Constitution. Under Article II, the President is given broad but vague authorities to act as Commander-in-Chief of the armed forces, make treaties, and "take care that the laws [of the United States] be faithfully executed." Under Article III, the judiciary is authorized to interpret and overturn statutes enacted into law, orders, and regulations issued by the executive branch. The judicial branch serves as the final arbiter of legality, with the Supreme Court providing a final check on the constitutionality of all authorities issued by the legislative and executive branches.

Of note, primary authorities, especially statutes and EOs, are often ambiguous. This is the case for a host of reasons, including:

- **Authorities cannot, and should not, be written to foresee and forestall every eventuality**. This would be futile: imagine the length of laws seeking to cover the waterfront. It would be impossible regardless, as the legislative process is too deliberative (even ponderous) to react in a timely fashion to evolving requirements and authorities cannot address the specific needs of all entities. Broad statutes and EOs provide a framework—but not necessarily a detailed roadmap—for the execution of responsibilities implicitly or explicitly vested in executive branch departments and agencies.

- Along these lines, **the emergence of new technologies may render existing authorities ineffective in achieving desired policy outcomes**. For example, authorities governing the regulation of the telecommunications sector have been found inadequate for newer technologies such as e-mail (not new in 2011, but new in historical context), requiring the development of updated authorities.[9] Indeed, in its *Cyberspace Policy Review,* the White House noted that "U.S. laws

[8] Primary and secondary authorities are discussed in the fields of constitutional and administrative law and executive power. For more on these fields generally, see, for example, Tribe (1999) as well as Stein and Mitchell (1990); for more on executive branch authorities and nuances therein, see, for example, Katyal (2006), Fisher (2007), Sunstein (2005), Relyea (2007a), and Reinstein (2009). For sources focused on national security and/or homeland security law, see, for example, Dycus et al. (2006), Moore and Turner (2005), and Nicholson (2005).

[9] For more on the need for updated authorities in response to the rapid adoption of the internet and coinciding technologies, see DOJ (2006). For a more recent discussion, see Kerry (2011). Examples of statutes written in part to address new technologies include the Computer Fraud and Abuse Act of 1986 and the Computer Security Act of 1987.

and policies governing cyberspace reflect serial attempts to keep pace with newly emerging challenges presented by the rapid technological and marketplace changes" (White House 2009a).

- **Judicial opinion may not yet exist (or exist in sufficient depth) to provide clear guidance on the proper interpretation of primary authorities**.[10] Alternatively, judicial opinion may exist, but its guidance may itself be indeterminate.[11] This is important not least because the power of the executive branch (particularly its ability to promulgate EOs) under the U.S. Constitution is vague; the absence of sufficient case law can foster a lack of clarity regarding the potential scope of executive powers.[12]

- Lastly, **the ability of the executive branch to mandate action by its constituent agencies without enabling legislation is uncertain**. This is particularly true in issues requiring activity outside of government, such as the regulation of private-sector entities.[13]

---

[10] The federal judiciary lacks independent authority to interpret a statute or regulation; it may only do so when a case is presented for adjudication.

[11] The delineation between the legislative and executive branches has been the subject of extensive debate and litigation, and the judiciary has vacillated on the scope of executive authority to respond to perceived risks to national security. The seminal case adjudicating the scope of executive authority is Youngstown Sheet and Tube Co. vs. Sawyer (343 U.S. 579 (1952)), which decided that "presidential powers are not fixed but fluctuate, depending upon their disjunction or conjunction with those of Congress." However, Youngstown failed to identify the breath of congressional authority toward the regulation of the executive, taking a narrower judgment against executive acquisition of private property.

[12] There has been substantial disagreement within the judiciary on this, including on the existence of presidential "completion power," which gives the executive branch substantial leeway in implementing statute (Goldsmith and Manning 2006). The primary area of dispute is whether the authority vested in the executive includes all powers not specifically restricted by the Constitution, or simply those specifically enumerated. The argument is not merely academic: the ability of the president to issue EOs was not codified by the framers, but has become an essential authority for the executive branch. Notes Relyea (2007b): "whether presidential directives have the force of law depends upon such factors as the President's authority to issue them, their conflict with constitutional or statutory provisions, and their promulgation in accordance with prescribed procedure."

[13] The day-to-day business of the executive branch is conducted largely through individual cabinet agencies, which are provided with the authority to promulgate rules and regulations affecting both internal operations as well as those of non-governmental entities under agency purview. Executive agencies derive their rulemaking authority from their respective enabling legislation; specific procedures to issue rules and regulations are derived from the Administrative Procedures Act (Pub.L. 79-404, 60 Stat. 237). For example, the Federal Energy Regulatory Commission (FERC) is empowered to regulate the energy sector, including taking punitive measures against privately-owned facilities in violation of federal rules. Similarly, DHS is provided with certain regulatory authorities, such as ensuring that chemical facilities adhere to the Chemical Facilities Anti-Terrorism Standards. Congress has the discretion to determine whether an administrative agency is given rulemaking authority. The legality of agency rulemaking under *Chevron* (*Chevron U.S.A. Inc. v. Natural Resources Defense Council, Inc.*,

C. Motivation for the Research

DHS has a central role to play in U.S. cybersecurity. But the primary authorities supporting and governing this central role appear to lack sufficient clarity (and depth). As a result, it remains difficult to judge their adequacy—and, more importantly, the fundamental nature and extent of the department's role in securing U.S. cyberspace.

That DHS authorities in cybersecurity appear to lack clarity and depth has been noted by numerous entities and individuals both within and outside of government. For example, the *Cyberspace Policy Review*, initiated at the behest of the Obama administration to conduct a clean-slate census of the national cybersecurity enterprise, determined that current authorities are "a patchwork of Constitutional, domestic, foreign, and international law … [that] may prompt proposals for a new legislative framework … or the application of new interpretations of existing laws" (White House 2009a).[14] Similarly, the seminal report of the Center for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency recognized the inadequacy of existing authorities, noting that "cyberspace has evolved continuously and quickly … this means that crucial authorities for better cybersecurity are increasingly outdated" (CSIS 2008).[15] A related follow-on report found that little progress had been made, stating that "the United States still lacks an integrated cybersecurity strategy" which can be overcome "if the nation passes laws and the administration issues effective regulations" (CSIS 2011).[16] And in its own *QHSR*, DHS reported a need to "develop, promulgate, and update guidelines, codes, rules, regulations, and accepted standards … that ensure the confidentiality, integrity, and availability of systems, networks, and data without impairing innovation, and while enhancing privacy" (DHS 2010d).

---

467 U.S. 837 (1984)) is largely dependent on whether Congress provided the agency with express or implied rulemaking authority. An EO directing a particular action by an agency may be legally unsustainable if not supported by statute (Sunstein 2005). Additionally, the federal courts have typically exercised substantial deference toward agency expertise regarding the interpretation of ambiguous legislation (Eskridge 2008).

[14] Indeed, an action in the near-term action plan of the *Cyberspace Policy Review* called for convening "appropriate interagency mechanisms to conduct interagency-cleared legal analyses of priority cybersecurity-related issues identified during the policy-development process and formulate coherent unified policy guidance that clarifies roles, responsibilities, and the application of agency authorities for cybersecurity-related activities across the Federal government" (White House 2009a).

[15] CSIS (2008) specifically discussed the need for improved authorities to broaden capabilities to collect electronic evidence, improve compliance standards for the Federal Information Security Management Act (FISMA), and remove artificial distinctions between certain civilian and national security systems. It also issued recommendations for new regulations to mandate the implementation of cybersecurity practices in government and private sector systems, particularly those affecting critical infrastructure.

[16] For a discussion of cybersecurity legislation debated during the 111th Congress, see Hathaway (2010). For a discussion of potential changes required in certain cyber-relevant statutes, see Hathaway (2011).

Government auditors have weighed in with similar conclusions. The Government Accountability Office (GAO) noted in an analysis of current DHS cyber capabilities that "the future position [of DHS cybersecurity entities] in the government's efforts to establish a national-level cyber analysis and warning capability is uncertain" (GAO 2008a). GAO additionally recognized the difficulty in coordinating cybersecurity activities across the federal government in the absence of clear authority, stating that "unless federal agencies institutionalize a coordination mechanism that engages all key federal entities, it is less likely that federal agencies will be aware of each other's efforts, or that their efforts, taken together, will support U.S. national interests in a coherent or consistent fashion" (GAO 2010a). At the DHS level, the Office of the Inspector General (OIG) found that the department lacks the authority to enforce compliance with cyber mitigations it recommends to other federal departments and agencies (Skinner 2010).

Likewise, Congressional Research Service authors have observed that "questions have arisen regarding the adequacy of legal authorities justifying executive responses to cyber threats … the current statutory framework likely does not address all potential actions" (Rollins 2009) and that "because of fragmentation of missions and responsibilities, 'stove-piping,' and a lack of mutual awareness between stakeholders, it is difficult to ascertain where there may be programmatic overlap or gaps in cybersecurity policy" (Theohary 2009).

Of course, certain documents do, in fact, discuss the authorities supporting and governing DHS cyber activities. The [interim] National Cyber Incident Response Plan (NCIRP; DHS 2010b) provides a comprehensive overview of particular roles and responsibilities across the homeland security enterprise during the response to a cyber event, and lists the authorities supporting the plan. However, the NCIRP does not correlate response roles and activities with the supporting authorities—and thus it does little to suggest whether existing authorities in fact support all elements of the current response plan.[17] The *Information Technology (IT) Sector Specific Plan* of the broader *National Infrastructure Protection Plan* provides an overview of authorities relevant to critical infrastructure protection in the IT sector. The aforementioned *BUR*, a census of DHS activities in support of *QHSR* mission areas, briefly outlines the current authorities supporting DHS cybersecurity activities, namely the Homeland Security Act of 2002 and NSPD-54/HSPD-23, but it does so without identifying the scope or limitations of such authorities.

Overall, a lack of clarity prevails. And this lack of clarity presents conditions for mission failure. This is the motivation for the present research.

[17] For a list of additional authorities related more generally to incident response, see Appendix 6 of the National Response Framework (DHS 2008).

D. Research Questions, Methodology, and Scope

This research sought to answer the following two questions:

- What are the primary authorities supporting/governing DHS efforts to secure U.S. cyberspace (and what do these authorities say)?
- What ambiguities, conflicts, and gaps appear to exist in these authorities, and what are their implications for the DHS mission?

To do so, the research team examined relevant literature (e.g., policy/legal/academic documents, media reports) on authorities, cyberspace, cybersecurity, homeland security, CIKR protection, information sharing, incident response, and the like. Examination of the literature was complemented by discussions with experts across the policy, legal, and academic communities both within and outside of DHS. Analysis of authorities focused on primary authorities (particularly statutes and EOs); secondary authorities were considered as appropriate.[18] The research was carried out on a part-time basis between December 2010 and March 2011.

Importantly, the research was conducted (and the document written) more from a policy perspective than a legal one. The document discusses germane issues of jurisprudence—such as executive power and the government's ability to intervene in private enterprise—but it seeks neither to formally settle them nor to extensively scrutinize their history. Rather, it seeks to highlight conceptual issues.

Further, while relevant classified authorities exist (e.g., NSPD-54/HSPD-23), the research examined only unclassified, publicly available information. This approach was chosen to gain an understanding of authorities from the perspective of the broader private sector, SLTTGs, and public at large. This perspective is important: private sector and SLTTG entities represent the first line of defense in the homeland security mission, and many, if not most, have no access to classified information.

Lastly, this research focused on the overarching cybersecurity efforts of DHS to secure civilian federal government computer systems and to coordinate security of SLTTG and privately owned systems. This has important implications for the scope of the research, including:

- DHS components have cybersecurity responsibilities that fall outside of this mandate. For example, Immigration and Customs Enforcement (ICE) investigates entities that sell counterfeit products via the internet, and initiates action against them. While this activity supports the overall homeland security mission, it falls outside the scope of the present paper and remains a topic for future research.

[18] Less attention was paid to agency-issued regulations (which are commonly viewed as primary authorities), because the research sought to understand and assess the authorities that grant DHS the power to work to secure U.S. cyberspace, not regulation DHS itself has promulgated.

- Given the focus on DHS, the research did not examine authorities that support and govern the efforts of other USG departments and agencies to secure national security systems (including the .mil and .ic domains).

- Numerous entities within the homeland security enterprise have their own primary authorities somehow relating to cybersecurity. For example, states commonly have data breach laws that require private entities to report breaches of customers' personal information. Such authorities are not discussed here.

- There is no perfect delineation separating authorities on cybersecurity from those on homeland security in general (or aspects thereof, like preparedness or response). This research focuses on authorities deemed by the authors to be of greatest relevance to DHS efforts to secure U.S. cyberspace; it excludes, however, certain authorities that may be considered more tangential. For example, Presidential Policy Directive-8 (PPD-8, National Preparedness, replacing HSPD-8) drives efforts to prepare for certain serious threats. While it notes that cyber attacks are included among threats posing greatest risk to the security of the United States, it does little to set forth specific DHS (or any other) activities in securing cyberspace. Such authorities are not discussed here.

III. PRIMARY AUTHORITIES

This chapter seeks to answer the first of the present paper's two research questions: "what are the primary authorities supporting/governing DHS efforts to secure U.S. cyberspace, and what do these authorities say." It presents a select list of primary authorities deemed by the authors to be most relevant to the efforts of DHS to secure U.S. cyberspace.[19] Authorities are addressed in Table 1 (next page) and the text below in two categories: those directly establishing the responsibilities of DHS to secure U.S. cyberspace, and those affecting DHS cybersecurity responsibilities. The implications of the select primary authorities are set forth in a discussion chapter that follows.

A. Authorities Establishing DHS Cybersecurity Responsibilities

The following primary authorities serve to establish DHS cybersecurity responsibilities.

National Security Presidential Directive 54/Homeland Security Presidential Directive-23 (2008)

NSPD-54 /HSPD-23 (Cyber Security and Monitoring) is a classified directive outlining the Comprehensive National Cybersecurity Initiative (CNCI), a series of goals to strengthen cybersecurity capabilities within the federal government and through collaboration with non-federal partners. While the present research did not review the classified version of NSPD-54 /HSPD-23, an unclassified redacted version is publicly available. It notes that the CNCI primarily focuses on the need to secure government networks, improve situational awareness across the cyber enterprise, and better define the role of the federal government in critical infrastructure domains. Particular authorities outlined in the CNCI include mandates for DHS to provide network assurance across the federal enterprise through secure network connections and intrusion detection and prevention systems, ensure interoperability and information sharing between federal cybersecurity operations centers, coordinate cybersecurity research and development initiatives across the federal enterprise, and increase collaborative efforts (including public-private partnerships) to improve the resiliency of critical infrastructure.

---

[19] The present paper discusses primary authorities that support and govern the efforts of DHS itself to secure U.S. cyberspace. It does not, however, discuss the universe of all authorities somehow, even tangentially, related to U.S. cybersecurity writ large (see p.8, "Research Questions, Methodology, and Scope," for a discussion of research scope). The following authorities were deemed to be outside the scope of the present paper: PPD-8: National Preparedness (2011); HSPD-20/NSPD-51: National Continuity Policy (2008); Protect America Act of 2007; E-Government Act of 2002; Sarbanes-Oxley Act of 2002; Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001; Gramm-Leach-Bliley Act of 1999; Health Insurance Portability and Accountability Act of 1996; Economic Espionage Act of 1996; Communications Assistance to Law Enforcement Act of 1994; National Security Directive 42: National Policy for the Security of National Security Telecommunications and Information Systems (1990); Foreign Intelligence Surveillance Act of 1978; Emergency Economic Powers Act of 1977; Foreign Corrupt Practices Act of 1977; National Security Act of 1947; and Securities Exchange Act of 1934.

Table 1. Primary Authorities of Relevance to the Efforts of DHS to Secure U.S. Cyberspace

Authorities establishing DHS cybersecurity responsibilities	***Year enacted (most recent revision)***
NSPD-54 /HSPD-23: Cyber Security and Monitoring	2008
HSPD-7: Critical Infrastructure Identification, Prioritization, and Protection	2003
EO 12472: Assignment of National Security and Emergency Preparedness Telecommunications Functions	1984 (2003)
EO 12382: President's National Security Telecommunications Advisory Committee	1982 (2003)
Homeland Security Act (HSA)	2002
Federal Information Security Management Act (FISMA)	2002
EO 13231: Critical Infrastructure Protection in the Information Age	2001
Authorities affecting DHS cybersecurity responsibilities	***Year enacted (most recent revision)***
Defense Production Act (DPA)	1950 (2009)
Computer Fraud and Abuse Act	1986 (2008)
EO 12333: United States Intelligence Activities	1981 (2008)
Stafford Act	1988 (2006)
Electronic Communications Privacy Act (ECPA)	1986 (2004)
Intelligence Authorization Act	2004
Intelligence Reform and Terrorism Prevention Act (IRTPA)	2004
HSPD-5: Management of Domestic Incidents	2003
Communications Act	1934 (1996)
National Emergencies Act	1976

Note: This table presents a select list of primary authorities deemed by the authors to be most relevant (see p. 8, "Research Questions, Methodology, and Scope," for a discussion of research scope).

Homeland Security Presidential Directive-7 (2003)

HSPD-7 (Critical Infrastructure Identification, Prioritization, and Protection) establishes "a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attack." HSPD-7 designates DHS as the coordinating agency for all (civilian) federal cybersecurity efforts, with the mandate to provide timely alerts, warnings, and analysis of emerging threats and vulnerabilities; to reduce and mitigate vulnerabilities; and to aid national recovery efforts for critical infrastructure systems. The directive also mandates that DHS support the FBI and other law enforcement partners in "investigating and prosecuting threats to and attacks against cyberspace."

Executive Orders 12472 and 12382 (as amended by EO 13286, 2003)

EO 12472 (Assignment of National Security and Emergency Preparedness Telecommunications Functions) codified the National Communications System (NCS), originally established in 1963 under Presidential Memo 252. EO 12472 mandates that

the NCS "incorporate the necessary combination of hardness, redundancy, mobility, connectivity, interoperability, restorability, and security into national telecommunications infrastructure necessary for national security and emergency preparedness capabilities under all conditions." EO 12382 (President's National Security Telecommunications Advisory Committee) established the National Security Telecommunications Advisory Committee to support the NCS with "information and advice from the perspective of the telecommunications industry with respect to the implementation [of the NCS] and … provide technical information and advice in the identification and solution of problems which the Committee considers will affect national security telecommunications capability." EO 13286 amended EOs 12472 and 12382 to transfer the NCS to DHS and designate the Secretary of DHS as the Executive Agent of the NCS.

Homeland Security Act (2002)

The Homeland Security Act (HSA) created DHS out of 23 disparate agencies and established missions and areas of responsibility for the particular components and offices. The HSA (6 U.S.C. §§143-144) mandates that DHS "develop a comprehensive national plan … and recommend measures necessary to protect key resources and critical infrastructure." It requires DHS, as appropriate, to provide technical assistance to private-sector owner-operators and help manage incidents affecting critical assets and information systems.[20] The HSA notes that the Secretary may "establish a national technology guard" to provide cybersecurity expertise to the private.[21] The HSA also authorizes information-sharing activities with other partners in the cybersecurity enterprise, including other federal agencies, state and local governments, and the private sector.

Federal Information Security Management Act (2002)

FISMA mandates that the Office of Management and Budget (OMB) reduce the risk of unauthorized access, use, disclosure, modification, or destruction of federal agency information or systems. FISMA (44 U.S.C. §3543 et seq.) tasks OMB with coordinating the interagency adoption of security practices and the development of control and monitoring systems for federal networks. FISMA additionally mandates that DHS cooperate with NIST to develop policies, procedures, and techniques for cybersecurity across government networks and systems. OMB issued subsequent guidance on FISMA implementation that authorizes DHS to both provide operational support to federal agencies in securing their systems and networks and monitor agency progress to ensure compliance with FISMA requirements (OMB 2010).

---

[20] The interim NCIRP (DHS 2010b) states that "an information system is considered to be critical if a physical or cyber incident affecting the confidentiality, integrity, and availability of the system, asset, or function would have significant negative impact on the national security, economic stability, public confidence, health, or safety of the United States."

[21] The "national technology guard" concept was the foundation for the development of the U.S. Computer Emergency Readiness Team (US-CERT).

Executive Order 13231 (2001)

EO 13231 (Critical Infrastructure Protection in the Information Age) assigns responsibilities for critical infrastructure protection (CIP), including cybersecurity, throughout the executive branch. Under EO 13231, the Director of OMB is responsible for developing and overseeing the implementation of government-wide policies, principles, standards, and guidelines for (civilian) federal information security. EO 13231 established the National Infrastructure Advisory Council (NIAC) to conduct outreach to the private sector and local governments; share information with critical infrastructure owner-operators; and coordinate programs and policies for responding to security incidents that threaten information systems for critical infrastructure, among other responsibilities. The NIAC is a standing body providing DHS with guidance and input from critical infrastructure owner-operators.

B. Authorities Affecting Established DHS Cybersecurity Responsibilities

Several primary authorities affect, in relevant ways, established (i.e., existing) DHS cybersecurity responsibilities. These are discussed below.

Defense Production Act of 1950 (as amended, 2009)

The Defense Production Act (DPA, 50 U.S.C. §2062, and §§2071-2077) authorizes the President, or a designee, to require that privately held firms prioritize the fulfillment of contracts with the federal government that are deemed necessary to "prepare for and respond to military conflicts, natural or man-caused disasters, or acts of terrorism," even if that prioritization involves the postponement or abrogation of other contracts. The DPA prioritization process allows the proactive allocation of materials, services, and facilities to ensure sufficient supplies are available as required for national defense or emergency. DPA also permits the President to mandate the increased use of emerging technologies in security program applications and the rapid transition of emerging technologies, from either government-sponsored or commercial research. To achieve the adoption of such technologies, the DPA also permits the provision of loans to "private business for the creation … or development of technological processes." The DPA statute additionally permits the President to mandate the modification or expansion of privately owned facilities, including the improvement of production processes, provides the federal government with full indemnity against any claims subsequent to the modification of privately owned facilities, and provides antitrust exemption for businesses to cooperate in supplying resources required for national defense.

Computer Fraud and Abuse Act of 1986 (as amended, 2008)

The Computer Fraud and Abuse Act (CFAA) criminalizes a variety of activities affecting "protected computers," defined as computers and systems operated by the federal government and financial institutions. CFAA (18 U.S.C. §1030) establishes criminal penalties for offenses relating to accessing "protected computers" without or in excess of express authorization, particularly unauthorized access to information protected for reasons of "national defense or foreign relations … or information to be used to the injury

of the United States or to the advantage of any foreign nation." The CFAA additionally imposes criminal penalties on unauthorized access to "information contained in a financial record of a financial institution" and defines a "federal interest computer" as both a computer used exclusively for government operations and a computer whose use affects government operations.

Executive Order 12333 (as amended, 2008)

EO 12333 (United States Intelligence Activities), among other things, authorizes the Director of National Intelligence to integrate applicable homeland and national security information or intelligence from all members of the intelligence community through the development of information sharing programs. EO 12333 also requires that the federal government incorporate the information needs of non-federal partners in the development of new information-sharing programs. EO 12333 outlines the roles and responsibilities of the respective components of the intelligence community, including DHS, and encourages the integration of SLTTGs and the private sector in applicable information sharing programs.[22]

Stafford Act (as amended, 2006)

The Stafford Act outlines the mechanisms and authorities through which the federal government provides support to SLTTGs after a disaster, either natural or man-made. Most authorities under the Stafford Act require an express request by the governor of the affected state and a finding that "the situation is of such severity and magnitude that effective local response is beyond the capabilities of State and affected local governments and Federal assistance is necessary." However, Section 501b of the Stafford Act (42 U.S.C. §5191) provides that the federal government may exercise authority over an emergency without a gubernatorial request when exclusive or preeminent responsibility resides at the federal level: "the President may exercise any authority vested in him with respect to an emergency when he determines that an emergency exists for which the primary responsibility for response rests with the United States because the emergency involves a subject area for which, under the Constitution or laws of the United States, the United States exercises exclusive or preeminent responsibility and authority."

Electronic Communications Privacy Act of 1986, including Title II, the Stored Communications Act (as amended, 2004)

The Electronic Communications Privacy Act of 1986 (ECPA, 8 U.S.C. §2511, 18 U.S.C. §§2516-18, §2515, and §§2701-12) amends Title III of the Omnibus Crime Control and Safe Streets Act of 1968 by expanding restrictions on the ability of law enforcement to monitor electronic communications, including email and internet traffic. The ECPA protects such communications from generation through deletion, including during storage and transit. ECPA prohibits interception, use, or disclosure of such transmissions unless expressly authorized by court order. Title II of the ECPA, known as the "Stored Communications Act," protects the data held by service providers, such as internet and

[22] See Lapointe (2010) for a discussion of the use, or not, of EO 12333 as a model for cybersecurity oversight.

telephone providers, and user-subscription records from unlawful acquisition and use (DOJ 2008).

Intelligence Acts (Intelligence Authorization Act for Fiscal Year 2004, Intelligence Reform and Terrorism Prevention Act of 2004)

Two intelligence acts in 2004 clarify DHS requirements for information sharing and analysis. The Intelligence Authorization Act for Fiscal Year 2004 (Title III Section 316) establishes requirements for DHS to better integrate the IC into existing information-sharing programs, in order to provide state and local governments and the private sector with timely threat information from all members of the IC. The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA; Subtitle A Sec. 102A and Subtitle D Sec. 7402) establishes the parameters for a single information-sharing environment (ISE) across the intelligence community. IRTPA mandates that the ISE "provide a means for sharing terrorism information among all appropriate Federal, State, local, and tribal entities, and the private sector, through the use of policy guidelines and technologies."

Homeland Security Presidential Directive-5 (2003)

HSPD-5 (Management of Domestic Incidents) authorizes DHS to coordinate federal efforts to prepare for, respond to, and recover from a terrorist attack or other major incident. Formally: "the Secretary shall coordinate the Federal Government's resources utilized in response to or recovery from terrorist attacks, major disasters, or other emergencies if and when any one of the following four conditions applies: (1) a Federal department or agency acting under its own authority has requested the assistance of the Secretary; (2) the resources of State and local authorities are overwhelmed and Federal assistance has been requested by the appropriate State and local authorities; (3) more than one Federal department or agency has become substantially involved in responding to the incident; or (4) the Secretary has been directed to assume responsibility for managing the domestic incident by the President." HSPD-5 also authorizes DHS to coordinate with the private and nongovernmental sectors to ensure adequate planning, and to promote partnerships to address incident management capabilities.

Communications Act of 1934 (as amended by the Telecommunications Act of 1996)

The Communications Act (47 U.S.C. §151 et seq.) authorizes the FCC to regulate the use of wire and radio communications in interstate and foreign commerce. Among other things, the Communications Act requires that every "telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to … carriers, manufactures and customers" unless disclosure was required by law or by customer request. The Communications Act also establishes the Network Reliability and Interoperability Council, replaced by the Communications Security, Reliability, and Interoperability Council, to provide guidance on system and service assurance for communications providers. Additionally, the Communications Act provides the President with the authority to suspend rules or regulations and order the closure of any

or all telecommunication stations or devices if deemed necessary during a state of war or national emergency.[23]

National Emergencies Act of 1976

The National Emergencies Act (50 U.S.C. §1601-1641) codifies the President's authority to declare a national emergency, which in turn triggers relevant statutes that require such a declaration for the exercise of executive authority. President George W. Bush declared a national emergency immediately subsequent to the 9/11 attacks; that declaration of a "National Emergency with Respect to Certain Terrorist Attacks" has been reissued every year since.[24] The current national emergency declaration has allowed the use of expanded surveillance powers against terrorism suspects (granted by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act and the Foreign Intelligence Surveillance Act, among others).

[23] For a detailed review of the history of modern communications technology and supporting legal frameworks, see White House (2009a), Appendix C. The ability of DHS to utilize the executive authorities of the Communications Act, as the designee of the President, during a cyber incident has been the topic of substantial debate and legal analysis (see the next chapter for further analysis of this issue).

[24] The National Emergencies Act does not explicitly define a national emergency, but states that "during the period of a national emergency, of any special or extraordinary power, the President is authorized to declare such national emergency."

IV. DISCUSSION

What, then, are the implications of the authorities discussed above? Does DHS truly "have the lead" for civilian federal government cybersecurity? And how does it "work with" SLTTGs and the private sector? Do authorities arm DHS with needed powers? Do they assign clear roles and responsibilities to cybersecurity actors within and outside of the USG? Or are they ambiguous, as suggested by previous authors, to the point where they may constrain the ability of DHS to secure U.S. cyberspace?

With such queries in mind, this chapter seeks to answer the second of the present paper's two research questions: "what ambiguities, conflicts, and gaps appear to exist in the relevant primary authorities, and what are their implications for the DHS mission." Ambiguities arise when primary authority language is vague or unclear (e.g., through the use of phrases like "coordinate" or "work with"), and may therefore limit the ability of DHS and others to effectively interpret their particular responsibilities in a given area. Conflicts arise when authorities appear to provide direction that either overlaps or is contradictory, and therefore may confuse agency responsibilities. Gaps arise when authorities provide direction but with obvious "distance" between specified responsibilities. Ambiguities, conflicts, and gaps—used here as heuristic devices—are analyzed by examining applicable language within the relevant primary authorities.

Through this analytical lens, the chapter highlights specific issues with the primary authorities supporting and governing the efforts of DHS to secure U.S. cyberspace. The chapter is not an exhaustive catalog, but rather a window into select issues. Issues are summarized below in Table 2 and discussed in greater detail in sections on system and information protection; information sharing; and incident response. These sections are based loosely on three important and related categories of activities in the cybersecurity life cycle:[25]

- *System and information protection* activities patch and protect against known or suspected vulnerabilities, block known or suspected threats, and detect incidents when they occur.
- *Information sharing* communicates the existence of known or suspected vulnerabilities and hostile IP addresses, etc. between and among communities of interest to ensure that systems and information are protected accordingly.
- *Incident response* ensures that the kinetic and nonkinetic effects resulting from cyber incidents are dealt with in a timely and appropriate manner to minimize physical, economic, and psychological costs to the nation, including loss of life. Some of the thorniest authorities-related issues fall in the category of incident response.

[25] As noted in footnote 5, see NIST (2010) and SANS (2009) for more information on specific cybersecurity activities.

Table 2. Issues Relating to Primary Authorities Supporting DHS Efforts to Secure U.S. Cyberspace

Category of activity	*Issue*
System/info protection	Existing authorities may not be fully sufficient for DHS to require or incentivize the protection of critical systems and information
Information sharing	Existing authorities may not be fully sufficient for DHS to collect information to be shared
Incident response	Existing authorities may not clearly define when DHS may intervene during a cyber incident
	Even when DHS may intervene, existing authorities may not fully support actions necessary to manage and coordinate cyber incident response
	Existing authorities expanding the power of the executive may be insufficient to allow DHS to require or incentivize needed action during the most serious of incidents
	Existing authorities may not sufficiently delineate the responsibilities of DHS and DoD during the most serious of incidents

A. System and Information Protection

System and information protection involves patching and protecting against known or suspected vulnerabilities, blocking known or suspected threats, and detecting incidents when they occur, thereby promoting security and resiliency. DHS has a role to play—granted by primary authorities—in the system and information protection of federal government and SLTTG and private-sector networks. Relevant language in the primary authorities includes the following (bold/italicized text is added for emphasis):

- HSPD-7: "[DHS shall] ***identify***, ***prioritize***, and ***coordinate*** the protection of critical infrastructure and key resources."
- HSPD-7: "[The DHS] mission ***includes*** vulnerability reduction [and] mitigation for critical infrastructure information systems."
- FISMA: "[NIST shall] ***promulgate*** information security standards pertaining to federal information systems."
- FISMA: "[OMB shall] ***require*** agencies to ***identify*** and ***provide*** information security protections commensurate with the risk and magnitude of the harm."

Analysis of the primary authorities suggests that **existing authorities may not be fully sufficient for DHS to require or incentivize the protection of critical systems and information**. Existing authorities clearly note that DHS maintains some level of responsibility in protecting systems and information, particularly relating to CIKR. Existing authorities are ambiguous, however. Using words like "identify," prioritize,"

"coordinate," and "provide," authorities notably do not specify that DHS has the ability to *direct* the adoption of specific mitigations or *mandate* the use of particular standards to reduce system vulnerability. Further, overlaps and conflicts in responsibility across the federal government may constrain the ability of DHS to develop, promulgate, and, where applicable, implement cybersecurity mitigations. These points are discussed in turn.

An OMB memorandum to federal government departments and agencies—based on the statutory authority of FISMA—requires that DHS "*provide* … operational support to federal agencies in securing federal systems [and] *monitor* and *report* agency progress" (OMB 2010). However, this guidance does not clarify whether DHS has the ability to *direct* specific actions to protect vulnerable systems when protection deficits are identified.[26] It is additionally unclear whether the federal government has an explicit responsibility to ensure the security of information systems supporting critical infrastructure (and the authorities supporting/governing DHS activities outside of the federal government appear to flow predominantly from DHS responsibilities to protect critical infrastructure), and if so, whether the owners of privately held systems can be *required* to adopt a specific mitigation if deemed critical to national security or defense. Current authorities may be insufficient to support overt government intervention in private networks, as they do not clearly define the lawful scope of government activities, resolve liability concerns, or provide a legal framework for compelling private-sector cooperation.[27] In an era of tight budgets, system operators may choose not to adopt otherwise appropriate system patches or other protective measures (perhaps because of market failure: their costs may outweigh perceived benefits for individual organizations). But such protective measures may be necessary to collectively effect strong cybersecurity in the United States. Absent an ability to direct or compel entities to take protective measures, DHS efforts to secure U.S. cyberspace may be lacking.[28]

---

[26] DHS OIG noted this concern in a 2011 report, finding that the U.S. Secret Service was non-compliant with agency cybersecurity requirements, in part due to the inability of DHS to require agency chief information officers to comply with department cybersecurity standards (DHS OIG 2011; see also Skinner (2010)).

[27] Similarly, these authorities may fail to clarify the extent to which DHS can recommend mitigations to the private sector, and whether any liability exists for either party, particularly if the mitigation leads to lost revenue or compromised proprietary information (Coldebella and White 2010). If the federal government maintains sovereign immunity from claims involving its recommended mitigations, it may discourage the adoption of DHS solutions (that is, if DHS recommends a vulnerability mitigation, like a software patch, that could result in some unintended system failure—with accompanying losses in revenue—private sector entities may not eagerly line up to take DHS advice unless there is some legal redress for potential losses). The U.S. authorizes suits to be brought against it through the Federal Tort Claims Act (FTCA). While there are several exemptions to the FTCA, it is uncertain whether the federal government would be liable in the case of failed (or malignant) cyber mitigation. For a discussion of the FTCA more generally, see Cohen (2007).

[28] Certain sector specific agencies (SSAs, the federal departments and agencies that oversee CIKR sectors) may utilize regulatory frameworks to mandate the adoption of mitigations by regulated entities under both legislative authority and directives such as EO 13286. However, the use of such regulations may not be fully integrated with DHS cybersecurity activities.

Further, although OMB guidance places requirements upon DHS to "monitor and report," it is unclear which entity maintains the responsibility to identify systemic vulnerabilities and propose or mandate solutions.[29] While DHS appears responsible for cybersecurity across federal government systems, NIST maintains statutory authority to develop security standards, with a mission to assist with implementation and ensure effectiveness. The presence of potentially conflicting responsibilities for system and information protection may limit the ability of DHS and its federal partners to effectively identify and resolve vulnerabilities in critical information systems.[30]

B. Information Sharing

Efforts to secure and defend systems and information rely heavily on the sharing of information on cyber threats and vulnerabilities. Information sharing strengthens the nation's cybersecurity posture by allowing cognizant entities to have the broadest possible understanding of known or suspected hostile IP addresses, potential exploits, etc. This information is shared between and among relevant communities of interest to ensure that systems and information are protected accordingly. Information sharing involves identifying information requirements, collecting actionable information, and disseminating it to those with a need to know and a capability to act.

DHS maintains responsibilities in cybersecurity information sharing. Relevant language in the primary authorities includes:

- HSA: "[DHS shall] ***provide*** … private entities that own or operate critical information systems [with] analysis and warnings related to threats to, and vulnerabilities of, critical information systems."
- HSPD-7: "[DHS shall] ***facilitate*** sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices."
- HSPD-7: "[DHS shall] ***establish*** appropriate systems, mechanisms, and procedures to share homeland security information relevant to threats and vulnerabilities in national critical infrastructure and key resources."
- IRTPA: "[The IC (of which the DHS Office of Intelligence & Analysis is a part) shall] ***ensure that*** [the ISE] provides and facilitates the means for sharing terrorism information among all appropriate Federal, State, local, and tribal entities, and the private sector through the use of policy guidelines and technologies."
- EO 12333: "[The IC] shall … ***facilitate***, as appropriate, the sharing of information or intelligence, as directed by law or the President, to State, local, tribal, and private sector entities."

[29] For a review of the legal issues underlying the deployment of DHS-managed intrusion detection systems on federal government networks, see Bradbury (2009).

[30] See footnote 20 for the definition of a "critical information system."

For context, relevant language from secondary (persuasive) documents includes:

- QHSR: "Information and intelligence regarding emerging cyber threats and vulnerabilities ***must be collected, analyzed, and shared*** appropriately and promptly."
- QHSR: "***Requires*** that ***sharing*** of information and analysis occur before malicious actors can exploit vulnerabilities."
- BUR: "DHS has the ***primary responsibility*** to share information and collaborate to enable understanding of the threat, provide indications and warnings, and create common situational awareness."
- BUR: "[DHS shall] ***collaborate*** and ***share*** cybersecurity information with critical infrastructure owners and operators, to enhance understanding of the threat, situational awareness, prevention, and incident response."
- NCIRP: "DHS ***provides*** a continuously updated, comprehensive picture of cyber threats, vulnerabilities, and consequences to provide…indications and warning of imminent incidents, and to support a coordinated incident response."

Analysis of the primary authorities suggests that while DHS undeniably plays a central role in facilitating cybersecurity information sharing, **existing authorities may not be fully sufficient for DHS to gather (i.e., collect) information to be shared**. That is, prevailing authorities do not specify whether DHS maintains the authority to require or otherwise incentivize relevant entities to report information to be shared (e.g., reports of suspicious activity and of both unsuccessful and successful cyber intrusions—and details thereof, like threat vector, vulnerability exploited, etc.) with DHS or some other information-sharing clearinghouse.[31]

Specifically, effective information sharing requires relevant, timely, and complete information. But existing statutes and directives may not provide DHS with sufficient

[31] Perhaps just as important, primary authorities do not spell out the *purpose and scope* of cybersecurity information sharing. This may be the nature of the beast: primary authorities are more strategic than tactical; as noted earlier in the present paper, they provide a framework, not a detailed roadmap. But if not in primary authorities, then where should purpose and scope be set forth? And without clear purpose and scope, it is difficult to understand what specific kinds of information should be shared, with whom, when, how, etc. High-level reviews of national cybersecurity efforts, such as the *Cyberspace Policy Review*, identify the need to define information sharing requirements (White House 2009a; and see also Coldebella and White (2010)). These are issues relating to the field of "data quality." Data quality is defined as "fitness for purpose." Data quality is typically measured along six dimensions: relevance, accuracy, timeliness/punctuality, accessibility/clarity, comparability, and coherence. Absent knowledge of the purpose to which data will be put, it is unlikely that data will be of sufficient quality to be of use. Lastly, note that there are existing restrictions of the ability of the executive branch to interfere with constitutionally protected interests. Such interference and interests have not been clearly defined in the cybersecurity domain. For further discussions of executive authority in the pursuit of national security interests more generally, see *Padilla v. Rumsfeld*, 2004.

authority to collect (and thus share) complete information.[32] This is the case because DHS appears unable to compel or otherwise incentivize sharing of complete relevant and timely information, even within the federal government. As such, DHS information sharing (and analysis) capabilities are entirely reliant on the voluntary provision of data (GAO 2008a).[33] While federal, non-federal, and private entities may fully support the reporting of threat and vulnerability information to DHS, they may, in practice, be constrained from doing so for various reasons.[34] For example, anecdotal evidence suggests that private-sector entities are reluctant to share certain information with the government because of perceived or actual liability issues; potential for loss of contracts (if the government is a customer); potential for impacts on reputation and/or stock price (should the information fall outside of the government's control); etc.[35] Absent the ability to compel or otherwise incentivize information sharing, DHS cannot ensure that information shared among and between public- and private-sector entities is representative of the overall cyber environment (i.e., DHS cannot ensure that it is complete).[36] Thus, its analytic products, threat signature feeds, etc. may be insufficient to secure U.S. cyberspace.[37]

---

[32] Primary authorities speak of DHS "providing" information and "facilitating" and "establishing" information sharing—but they do not specify the provenance of information to be shared.

[33] The HSA defines such voluntary information reporting: "the submittal thereof in the absence of such agency's exercise of legal authority to compel access to or submission of such information and may be accomplished by a single entity or an Information Sharing and Analysis Organization on behalf of itself or its members."

[34] A recent DHS white paper outlining the concept of a "cyber ecosystem" implicitly contains similar requirements for automated sharing of information to enable rapid identification of threats and vulnerabilities to inform a "self-healing" system. For additional discussion, see Herrera-Flanigan (2011) and DHS (2011).

[35] The *Cyberspace Policy Review* notes this concern, and outlines an integrated approach to incentivizing information sharing including the use of regulatory measures, data breach notification laws, and a bottom-up review of existing policies toward the use, retention and dissemination of potentially sensitive information.

[36] The federal government may be constrained by law from accessing or monitoring privately held data. The ECPA (including the Stored Communications Act) requires that the government receive judicial authorization prior to mandating the disclosure of electronic communications, possibly creating an elevated burden to compel the disclosure or submission of cybersecurity information. Additionally, the CFAA sets forth protective measures, including criminal penalties for unauthorized access to a "protected computer" (defined as computers and systems used for national security or foreign relations, storing the financial records of financial institutions, or the exclusive use of the federal government). This definition of a "protected computer" is narrower than the definition of a "critical information system" set forth in the interim NCIRP (and the definition of a "critical information system" does not appear to be supported by existing authorities, a gap that is addressed in the White House Cybersecurity Legislative Proposal released in May 2; see White House, 2011a). Separately, it is additionally unclear how DHS information-sharing responsibilities overlap or conflict with similar entities, including the ISE established through IRTPA.

[37] Information sharing seeks, among other things, to provide situational awareness. An incomplete picture of the environment—incomplete because of only partial information sharing—implies only partial situational awareness.

Interestingly, the language of the QHSR, BUR, and NCIRP suggests a stronger role for the department. While primary authorities speak of "providing," "facilitating," and "establishing," the QHSR, BUR, and NCIRP speak of "requiring" and "providing continuously updated comprehensive pictures."

C. Incident Response

Preventing all cyber incidents is impossible. Cyber incident response can help ensure that the kinetic and nonkinetic effects of cyber incidents that do happen are dealt with in a timely and appropriate manner to minimize physical, economic, and psychological costs to the nation. Effective cyber incident response requires the ability to be made aware of relevant incidents; to assist, as necessary, with technical fixes to restore affected systems and information; and to assess, respond to, and recover from broader kinetic and nonkinetic effects, not least physical damage.

DHS plays a central role in cyber incident response. Relevant language in the primary authorities supporting and governing DHS in cyber incident response includes:

- HSPD-7: "[The DHS mission includes] ***aiding*** national recovery efforts for critical infrastructure information systems."
- HSA: "[DHS] ***may establish*** a 'national technology guard' to ***assist*** local communities to respond and recover from attacks on information systems and communications networks."
- HSA: "[DHS shall] ***provide*** crisis management support in response to threats to, or attacks on, critical information systems."
- HSA: "[DHS shall] ***provide*** technical assistance, upon request, to the private sector and other government entities … with respect to emergency recovery plans to respond to major failures of critical information systems.
- HSPD-7: "[OMB] will ***ensure*** the operation of a central Federal information security incident center."
- HSPD-5: "[DHS] will ***coordinate*** with the private and nongovernmental sectors to ***ensure*** adequate planning [and] ***promote*** partnerships to address incident management capabilities."
- HSPD-5: "[DHS] is responsible for ***coordinating*** Federal operations within the United States to ***prepare for, respond to, and recover*** from terrorist attacks, major disasters, and other emergencies. The Secretary shall ***coordinate*** the Federal Government's ***resources***…if and when any one of the following four conditions applies: (1) a ***Federal department*** or agency acting under its own authority has ***requested*** the assistance of the Secretary; (2) the resources of ***State and local authorities*** are ***overwhelmed*** and Federal ***assistance*** has been ***requested*** by the appropriate State and local authorities; (3) ***more than one Federal department*** or agency has become substantially involved in ***responding***

to the incident; or (4) the ***Secretary*** has been ***directed*** to assume responsibility for managing the domestic incident ***by the President***."

For context, relevant language from secondary DHS documents includes:

- NCIRP: "[DHS is] ***responsible*** for ***providing*** crisis management and coordination in response to Significant Cyber Incidents."
- QHSR: "[DHS must] ***manage*** cyber incidents from identification to resolution in a rapid and replicable manner with prompt and appropriate action."
- NCIRP: "All Federal organizations ***must provide*** information on their ongoing cyber-related operations ***to the extent permitted by law*** to inform the common operational picture and assist coordination and deconfliction efforts."
- National Infrastructure Protection Plan: "[DHS] will ***provide*** crisis management in response to incidents involving cyber infrastructure."
- BUR: "DHS is ***responsible*** for ***creating*** and ***maintaining*** a robust public-private cyber incident response capability to manage cyber incidents from identification to resolution in a rapid and replicable manner with prompt and appropriate action."

Four issues of note relate to DHS authorities supporting and governing cyber incident response. These are discussed in turn, below.

First, analysis of the primary authorities suggests that **existing authorities may not clearly define when DHS may intervene during a cyber incident**. Primary authorities explicitly state that DHS is required to intervene during *certain* cyber incidents, particularly those affecting critical information systems. However, these authorities do not appear to require DHS to provide proactive support to *all* cyber incidents. Indeed, many common e-mail scams (e.g., "phishing") or individual network probes (of which there are millions per day) likely do not merit direct DHS intervention, save for potential collection of certain incident information (for sharing with the cyber community; see the section on information-sharing, above). While DHS is mandated in HSPD-5 to provide assistance during an incident that reaches a particular threshold of consequences, the definition and characteristics of such an incident have not been codified in primary authority. This ambiguity may limit the ability of DHS to clearly define when its capabilities are required, and therefore may constrain the development of appropriate mechanisms for response.

The interim NCIRP—a secondary authority—notes that DHS is "responsible for providing crisis management and coordination in response to Significant Cyber Incidents." A "significant cyber incident" is defined as an elevation of the National Cyber Risk Alert Level (NCRAL) to level 2.[38] However, it is unclear whether this

[38] Level 2 of the NCRAL is described as a cyber incident that "includes the observed or imminent degradation of critical functions with a moderate to significant level of consequences, possibly coupled with indicators of higher levels of consequences" (DHS 2010b).

threshold is clearly aligned with existing primary authorities. The HSA mandates that DHS provide "crisis management and support" to critical information systems, but the NCIRP is ambiguous regarding whether a level 2 NCRAL determination is considered a "crisis" under the HSA. Similarly, HSPD-5 relies upon specific conditions that may or may not be triggered during a cyber incident. It is unclear how the government would determine whether HSPD-5 conditions had been satisfied, particularly if there is a lack of clear information regarding incident scope. HSPD-5 additionally notes that DHS intervention on federal systems is limited to situations in which "a Federal department or agency acting under its own authority has *requested* the assistance of the Secretary" (emphasis added). This language implies that if a federal agency chooses not to request DHS assistance, the department has no authority to directly intervene unless so ordered by the President. Although the NCIRP appears to outline basic criteria for determining whether the need for DHS intervention to a cyber incident exists, primary authorities are unclear as to whether intervention would be supported if the requirements of a given statute (e.g., definition as a "crisis," fulfilling HSPD-5 requirements for DHS leadership, or the express request of a federal agency) are not met.

Second, analysis suggests that **even when existing authorities provide DHS with *responsibility* to intervene during a cyber incident, they may not fully support actions necessary to manage and coordinate cyber incident response**.[39] This issue exists primarily because of ambiguity surrounding the extent to which DHS may *require* or otherwise incentivize affected entities—whether federal, non-federal, or private—to provide incident information and adopt DHS-recommended mitigations once an incident has occurred.[40] That is, even in response to a "significant cyber event," it is unclear if DHS has the authority to *actually* intervene. This overall issue is similar to those discussed in sections above on system and information protection and information sharing. The nuance here is the focus specifically on incident response (i.e., cybersecurity activity that is directed at mitigating the results of an incident that has already taken place, not on proactive or ex ante protective measures).

For example, the HSA requires DHS to provide assistance after an incident affecting a critical information system. However, this authority can only be exercised "upon request" of the system owner. While in many cases the assistance of the government may be readily requested and appreciated, in some cases, certain entities may choose to decline assistance, or even hide the existence of an incident. This is the case because such entities may be: concerned about how a cyber incident would affect their reputation; hesitant to grant government access to proprietary or confidential information; or even overconfident in their internal consequence management procedures (see page 22 for

[39] According to the interim NCIRP, DHS responsibilities include, in part, the assessment of damage and vulnerabilities as well as the development of mitigations to limit incident consequences and restore critical functions.

[40] DHS has the stated responsibility under the NCIRP to manage and coordinate the response to a cyber incident. The authorities supporting the NCIRP appear to include both HSPD-5—which gives DHS the statutory responsibility to coordinate the federal response to a terrorist attack, major disaster, or other emergency—and HSPD-7, which authorizes DHS to "serve as the focal point" for ensuring a secure cyberspace.

similar views).[41] If government assistance is not directly requested, DHS does not appear to have authority to intervene.[42] A similar issue was noted by the DHS OIG, which reported that DHS lacked authority to require federal agencies to report cyber incidents (DHS OIG 2007; this is also referenced above in the section on information sharing). DHS policy documents note that the department should "manage cyber incidents" (QHSR) and "manage cyber incidents from identification to resolution" (NCIRP). In order to *manage* a cyber incident, DHS requires the ability to collect incident information as it occurs, and ensure that effective solutions are adopted to expedite incident resolution and minimize consequences. Primary authorities may not fully support this ability.

The third incident response issue relates to the expansion of executive power in the most serious of circumstances. Although existing authorities do not specify the scope of executive authority during a cyber incident, the President does possess the capability to exercise expanded powers during an incident deemed a threat to the interests of the United States. Existing authorities to expand the scope of federal powers were initially developed for the exigencies of an act of war or insurrection, and gradually expanded to encompass natural disasters and terrorist attacks.[43] Relevant language in primary authorities regarding the expansion of power includes:

- Stafford Act: "The President may ***exercise any authority*** vested in him with respect to an emergency when he determines that an emergency exists for which the primary responsibility for response rests with the United States because the emergency involves a subject area for which, under the Constitution or laws of the United States, the United States exercises exclusive or preeminent responsibility and authority."

- DPA: "[As required for the national defense] the President may ***require the modification or expansion*** of privately owned facilities, including the modification or improvement of production processes."

- Communications Act: "Upon proclamation by the President that there exists war or a threat of war, or a state of public peril or disaster or other national emergency, or in order to preserve the neutrality of the United States, the President, if he deems it necessary in the interest of national security or defense,

[41] The USA PATRIOT Act and precursor statutes such as Communications Assistance to Law Enforcement Act and the ECPA specifically prohibit the acquisition of any personal or proprietary data without express judicial authorization. It is unclear how this might affect DHS incident response.

[42] Of course, unlike a purely kinetic natural disaster or traditional terrorist attack, it may not be immediately evident to DHS that a cyber attack has occurred if the department is not notified by affected parties.

[43] These statutes were originally developed to both maximize the resources available for a response to an existential threat, as well as protect the citizenry from the unnecessary exercise of government authority. The executive branch has used these authorities in a variety of situations. For example, the DPA was utilized to restore rail service to the Gulf Coast after Hurricane Katrina and the National Emergencies Act was applied after 9/11, and subsequently reauthorized each year, to expand the legal scope of certain federal law enforcement activities (GAO 2008b).

may ***suspend or amend***, for such time as he may see fit, the ***rules and regulations*** applicable to any or all stations or devices."

- National Emergencies Act: "During the period of a national emergency, of any special or extraordinary power, the President is authorized to declare such national emergency."

While authorities exist permitting the broad expansion of executive powers to intervene during the most serious of incidents, including incidents affecting the national security or defense of the United States, analysis suggests that **existing authorities expanding the power of the executive branch may be insufficient to allow DHS to require or incentivize needed action for the most serious of cyber incidents**.[44] These expansionary primary authorities were designed to provide the President with the capability to take exceptional action deemed necessary to the national interest. The criteria for the use of existing statutes to expand the power of the executive were left intentionally vague, to allow the President flexibility in exercising those powers authorized by the legislature (Relyea 2007a). This intentional ambiguity has allowed a wide range of uses for these expanded authorities. However, as discussed above, the critical action required during a cyber incident is the acquisition of incident information and the adoption of effective mitigations by affected entities, either by compulsion or incentive. While expanded authorities provide a broad scope for potential action, it is unclear if they permit specific activities necessary to manage and coordinate a cyber incident response.

These expanded authorities are generally used to expand the powers of the federal government in areas where they would usually be prohibited. For example, the Stafford Act enables federal intervention in areas traditionally under the purview of state or local government. Similarly, the DPA was designed to allow federal intervention into the private sector, and the Communications Act allows the President to directly regulate the telecommunications network in a time of war. The National Emergencies Act provides perhaps the broadest powers, allowing the President to exercise expansive powers (within Article II boundaries) to ensure national security and defense. However, even these escalated powers may not provide the executive branch with the authority to require the submission of incident information or the adoption of mitigations.

Although the Stafford Act allows federal intervention during a "major emergency," this capability traditionally involves the direct provision of aid or resources—there is no precedent for the use of Stafford to compel direct action, even when the incident directly

[44] Generally, action has been taken when the specific exigencies of a recent incident require increased authorities. For example, the National Emergencies Act was utilized after 9/11 to expand the resources available to DoD and invoke emergency economic powers against suspected terrorist supporters (Relyea 2005). The Stafford Act has been utilized to provide significant federal assistance to areas affected by natural disaster. However, this assistance is predicated upon an express request by the governor of an affected state, or a presidential declaration that the incident affects primarily federal interests.

affects federal interests.[45] The DPA has been used to compel action by the private sector, but the legality of using this statute during a cyber incident is unknown—as it is not clear if a cyber mitigation falls within the statutory language of "modification or expansion." The Communications Act has the potential to be used for managing the consequences of a rapidly spreading cyber incident, under the President's power to control the transmission of telecommunications. While the NCS establishes a framework (codified in EO 12472) for the President to ensure the provision of national security or emergency preparedness telecommunications, it is unclear whether the pre-internet language of the Communications Act is directly analogous to modern communications (for example, does the authority to restrict radio transmission permit restricting internet service providers?).[46] The response to a cyber incident, particularly one involving cascading effects, must be nearly instantaneous. Ambiguous guidance regarding the application of expanded federal authority therefore may constrain the expedited deployment of needed mitigations across critical information systems. Although effective authorities may exist to expand the power of the executive during an incident affecting U.S. national interests, it is unclear whether these authorities can be exercised in a meaningful way during a cyber incident, and if their use will permit the government to effectively manage such an event.

Lastly, a sub-issue of relevance falls under the subject of response to an incident affecting U.S. national security or defense: who is responsible for what. Through its U.S. Cyber Command (USCYBERCOM), a sub-unified command under U.S. Strategic Command, DoD monitors and defends military systems and information (the .mil domain).[47] DoD works closely with DHS, as described by Deputy Secretary of Defense William Lynn: "the Pentagon is now working with the Department of Homeland Security to protect

---

[45] Under the Stafford Act, "*'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. *'Major disaster'* means *any natural catastrophe* (including any hurricane, tornado, storm, high water, winddriven water, tidal wave, tsunami, earthquake, volcanic eruption, landslide, mudslide, snowstorm, or drought), or, regardless of cause, any fire, flood, or explosion, in any part of the United States, which in the determination of the President causes damage of sufficient severity and magnitude to warrant major disaster assistance under this Act to supplement the efforts and available resources of States, local governments, and disaster relief organizations in alleviating the damage, loss, hardship, or suffering caused thereby" (emphasis added).

[46] Such a mechanism, which refines authorities under the Communications Act to provide the President with limited powers to segregate affected systems from the broader internet, is included in several draft cybersecurity bills in the 112th Congress, including S.3480 proposed by Sens. Lieberman and Collins.

[47] Recognizing the expertise and unique capabilities residing in DoD, a memorandum of agreement was issued in September, 2010 that "increased interdepartmental collaboration in strategic planning for the Nation's cybersecurity, mutual support for cybersecurity capabilities development, and synchronization of current operational cybersecurity mission activities" between DHS and DoD (DHS 2010c). Separately, note also that incident authorities for both DoD and civilian agencies may be expanded under an authorization for the use of military force (AUMF). Executive discretion to interpret ambiguous legislation may greatly increase under an AUMF. For differing perspectives on the boundaries of executive authority under an AUMF, see Bradley and Goldsmith (2005), as well as Sunstein (2005).

government networks and critical infrastructure and with the United States' closest allies to expand these defenses internationally" (Lynn 2010). However, analysis suggests that **existing authorities may not sufficiently delineate the responsibilities of DHS and DoD for the most serious of incidents, including incidents affecting the national security or defense of the United States**. This paper is by no means the first to point this out; the issue is identified here for completeness.

DoD directives authorize support to civil authorities when "such activities are necessary to prevent significant loss of life or wanton destruction of property and are necessary to restore governmental function and public order; or, when duly constituted Federal, State, or local authorities are unable or decline to provide adequate protection for Federal property or Federal governmental functions" (DoD 2010).[48] Such authorization may permit direct DoD intervention to limit the consequences of a cyber event that "seriously endangers life and property and disrupts normal governmental functions" (DoD 1989). Yet the parameters and triggers for such intervention remain ill-defined and present policy, legal, and constitutional concerns.[49] Indeed, General Keith Alexander, commander of USCYBERCOM and Director of the National Security Agency, recently stated explicitly that "[my] mission as the Commander of US Cyber Command is to defend the military networks. That's what authority I have today. I do not have the authority to look at what's going on in other government sectors nor what would happen to critical infrastructure" (Alexander 2011). DoD may be best resourced to prevent and limit the scope of a catastrophic cyber event.[50] However, existing authorities appear to provide neither a clear definition of the DoD role, nor the permissible scope of DoD intervention in non-military cybersecurity.[51]

---

[48] For additional information regarding the cyber capabilities of DoD, see Owens (2009).

[49] For example, the use of military assets requires express congressional authorization within 48 hours under the War Powers Resolution. The expedited nature of a cyber response means that Congress may be unable to "play a meaningful contemporaneous role" in providing its constitutional oversight and consent (Dycus 2010). The legal ramifications of such an occurrence have not been adjudicated or resolved.

[50] Additionally, U.S. Northern Command (USNORTHCOM) "anticipates and conducts Homeland Defense and Civil Support operations within the assigned area of responsibility to defend, protect, and secure the United States and its interests" (DoD 2007). USNORTHCOM may have a significant role in the response to a cyber incident, particularly regarding the management of kinetic impacts. However, the cybersecurity responsibilities of USNORTHCOM may be unclear, particularly its role vice USCYBERCOM and DHS.

[51] Indeed, the ability of DoD to intervene during a cyber incident may be constrained by existing statute. The President is specifically prohibited under the Posse Comitatus Act from utilizing military assets for the "purpose of executing the laws except in such cases and under such circumstances as … expressly authorized by the Constitution or by act of Congress." The vague language of Posse Comitatus may preclude DoD intervention during a cyber incident, particularly if the incident response is conducted in cooperation with Title 18 authorities. Some statutes do exist to allow DoD intervention in domestic events; for example, the Insurrection Act of 1807 provides the President with authority to utilize the armed forces to suppress any "insurrection, domestic violence … or conspiracy if it opposes or obstructs the execution of the laws of the United States or impedes the course of justice under those laws." Language in the 2007 National Defense Authorization Act expanded the scope of the Insurrection Act to allow

These issues raise salient questions regarding the ability of DHS to effectively lead a national response to cyber incident. For example, the language of the DPA indicates that it can be used to require modifications of private facilities in the service of national defense; can this authority be used to mandate the application of patches or other mitigations to reduce consequences of an evolving cyber threat? Moreover, what is the level of kinetic damage required to permit the intervention of the armed forces to assist with incident attribution and management? At what point do the incident response capabilities of DHS defer to those of DoD, and does the statutory role of DHS conflict with the mission and capabilities of USCYBERCOM? The role of DHS as the "focal point" of securing U.S. cyberspace is most essential when critical functions are jeopardized by a cyber incident. A cyber incident with the potential to jeopardize the security, prosperity, or livelihood of the United States requires an integrated response between civilian and military capabilities, a response which may be constrained without unambiguous authorities and defined legal responsibilities.

the use of the armed forces during a "natural disaster, epidemic, terrorist attack or other condition"; however, this clause was repealed in 2008 to again restrict DoD intervention to an act of war or insurrection.

V. Conclusions and Thoughts for Future Research

This paper examined DHS-related cybersecurity authorities and sought to understand their broad implications on the responsibilities of DHS in securing U.S. cyberspace. Overall, the research suggests that existing DHS-related authorities may not be fully sufficient for DHS to: require or incentivize the protection of critical systems and information; gather (i.e., collect) information to be shared; define clearly when DHS may intervene during a cyber incident; support actions necessary to manage and coordinate cyber incident response, including for the most serious of incidents; and delineate the responsibilities of DHS and DoD for the most serious of incidents.

Notable avenues for future research exist. Most importantly, the paper did not explore—in any depth—the specific authorities of DoD in securing U.S. cyberspace. Comparing DoD authorities to those of DHS would facilitate understanding of the broader landscape, given the centrality of the two departments to the overall mission. Also, a similar analysis of the authorities of states (and local/tribal/territorial entities), and of the responsibilities (e.g., mandatory incident reporting) placed on private sector entities, would shed additional light on the environment, as would an examination of the authorities supporting the specific cyber-related law enforcement activities of DHS components like ICE, U.S. Secret Service, and Customs and Border Protection. Lastly, several cybersecurity bills, including legislation sponsored by Sens. Lieberman and Collins (as well as proposed legislative language transmitted to Congress by the White House in May 2011, which may or may not find its way into bills), have been proposed in recent months. A useful endeavor would be to consider the conclusions of the present paper alongside specific components of proposed legislation. These remain topics for the future.

Finally, while the present research did not seek to understand *why* ambiguities, conflicts, and gaps persist in current authorities, it seems reasonable to consider that rapid technology evolution and adoption, particularly of networked systems (including industrial control systems) and decentralized data storage (cloud storage), have created novel cybersecurity risks that have outpaced the scope of existing authorities (for a similar view, see CSIS (2011), among others). Further, the authorities that currently govern and support DHS cybersecurity activities have primarily grown in response to kinetic threats, particularly those imposed by terrorists armed with more "traditional" non-cyber weapons—and cyber may be sufficiently different that authorities designed to cope with traditional threats are inherently incapable of responding to the novel threat profile. But perhaps what is most important in understanding why ambiguities, conflicts, and gaps persist is the fact that the United States has not yet knowingly faced a "cyber-Hurricane Katrina." After all, the impetus for reform is often spurred by a major event that reveals the shortcomings of an existing system. After Katrina devastated New Orleans in 2005, a bipartisan task force recommended wholesale changes to the authorities and responsibilities supporting the federal role in incident management and response; many of these recommendations were rapidly codified in legislation. Although cybersecurity is an omnipresent concern for security professionals, and significant cyber

incidents—from Stuxnet to massive death-by-a-thousand-cuts intellectual property data thefts—have elevated the profile of cybersecurity's importance, there has not yet been an incident that raises the issue of cybersecurity to a top national priority. Those departments and agencies responsible for preventing, detecting, and responding to a significant cyber event—not least DHS—must have the tools and authorities necessary to lean forward and minimize both the likelihood and the consequences of such a cyber incident—before one happens.

ACRONYMS

BUR	Bottom-Up Review Report
CFAA	Computer Fraud and Abuse Act
CIKR	Critical infrastructure/key resources
CNCI	Comprehensive National Cyber Initiative
CSIS	Center for Strategic and International Studies
DHS	Department of Homeland Security
DoD	Department of Defense
DPA	Defense Production Act
ECPA	Electronic Communications Privacy Act
EO	Executive order
FCC	Federal Communications Commission
FERC	Federal Energy Regulatory Commission
FISMA	Federal Information Security Management Act
GAO	Government Accountability Office
HSA	Homeland Security Act
HSI	Homeland Security Studies and Analysis Institute
HSPD	Homeland Security Presidential Directive
IC	Intelligence community
IP	Internet protocol
IRTPA	Intelligence Reform and Terrorism Prevention Act
ISAC	Information sharing and analysis center
ISE	Information sharing environment
NCIRP	National Cyber Incident Response Plan
NCRAL	National Cyber Risk Alert Level
NCS	National Communications System
NIST	National Institute of Standards and Technology
NSPD	National Security Presidential Directive
OIG	Office of the DHS Inspector General
OMB	Office of Management and Budget
PD	Presidential directive
QHSR	Quadrennial Homeland Security Review
SLTTG	State, local, tribal, and territorial governments
U.S.	United States
U.S.C.	United States Code
US-CERT	U.S. Computer Emergency Readiness Team
USCYBERCOM	U.S. Cyber Command
USG	United States government
USNORTHCOM	U.S. Northern Command

REFERENCES

Ackerman, Bruce. 2004. "The Emergency Constitution." *Yale Law Journal* 113: 1031-1091.

Addicon, Jeffrey F. 2007. *Terrorism Law: Materials, Cases, Comments.* Tucson, AZ: Lawyers and Judges Publishing.

"Administrative Procedures Act," 5 U.S.C., §§ 500-596.

Alexander, Keith. 2011. "Cyber Symposium Keynote Address." University of Rhode Island. Kingston, RI: April 11.

Barron, David J., and Martin S. Lederman. 2008. "The Commander in Chief at the Lowest Ebb: Framing the Problem, Doctrine and Original Understanding." *Harvard Law Review* 3: 689-801.

Blair, Dennis C. 2009. Director of National Intelligence, to Senators Feinstein and Bond. May 19.

Bradbury, Steven G to Fred F. Fielding, Counsel to the President. 2009. *Memorandum Regarding Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection System (EINSTEIN 2.0) To Protect Unclassified Computer Networks in the Executive Branch.* January 9.

Bradley, Curtis A. and Goldsmith, Jack L. 2005. "Congressional Authorization and the War on Terrorism." *Harvard Law Review* 118: 2048-2132.

Cashell, Brian et al. 2004. *The Economic Impact of Cyber-Attacks.* Washington, DC: Congressional Research Service.

Cauley, Gerry. 2011. "Remarks of the President and CEO, North American Electric Reliability Corporation." Testimony before the House Armed Services Committee. February 11.

Center for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency. 2011. *Cybersecurity Two Years Later*. Washington, DC: CSIS.

———. 2008. *Securing Cyberspace for the 44th Presidency*. Washington, DC: CSIS.

Chemerinsky, Erwin. 2006. "The Assault on the Constitution: Executive Power and the War on Terrorism." *UC Davis Law Review* 40: 1-20.

Chevron, U.S.A., Inc. v. Natural Resources Defense Council. 467 U.S. 837 (1984).

Clarke, Richard A., and Robert K. Knake. 2010. *Cyber War: the Next Threat to National Security and What to Do about It*. New York: Ecco.

Cohen, Henry, and Vanessa K. Burrows. 2007 (updated). *Federal Tort Claims Act.* Washington, DC: Congressional Research Service.

Coldebella, Gus P. and Brian M. White. 2010. "Foundational Questions Regarding the Federal Role in Cybersecurity." *Journal of National Security Law and Policy* 4: 233-245.

Committee on National Security Systems (CNSS). 2010. *National Information Assurance Glossary*. Washington, DC: CNSS.

"Communications Act of 1934, as amended," 47 *U.S.C.,* §60.

"Communications Assistance for Law Enforcement Act of 1994," 47 *U.S.C.,* §§102, 103, and 105.

"Computer Fraud and Abuse Act of 1986," 18 *U.S.C.,* §1030.

"Computer Security Act of 1987," 15 *U.S.C.,* §§271-278."Defense Production Act of 1950," 50 *U.S.C.,* §§2062, 2071, and 2077.

Department of Defense (DoD). 2010. "Defense Support of Civil Authorities." DoD Directive 3025.18. Washington, DC: DoD.

———. 2007. *NORAD and U.S NORTHCOM Vision 2020.* Washington, DC: DoD.

———. 1989. *DoD Cooperation with Civilian Law Enforcement Officials*. DoD Directive 5525.5 (Encl. 4) Washington, DC: DoD.

Department of Homeland Security (DHS). 2011. *Enabling Distributed Security in Cyberspace.* Washington, DC: DHS.

———. 2010a. *Bottom-Up Review Report*. Washington, DC: DHS.

———. 2010b. *Interim National Cyber Incident Response Plan*. Washington, DC: DHS.

———. 2010c. *Memorandum between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity.* Washington, DC: DHS.

———. 2010d. *Quadrennial Homeland Security Review*. Washington, DC: DHS.

———. 2009a. *National Infrastructure Protection Plan*. Washington, DC: DHS.

———. 2009b. *Roadmap for Cybersecurity Research.* Washington, DC: DHS

———. 2008. *National Response Framework.* Washington, DC: DHS.

———. 2007. Information Technology Sector Specific Plan. Washington, DC: DHS

Department of Homeland Security Office of the Inspector General (DHS OIG). 2011. *U.S. Secret Service's Information Technology Modernization Effort.* Washington, DC: DHS.

———. 2007. *Challenges Remain in Securing the Nation's Cyber Infrastructure*. Washington, DC: DHS.

Department of Justice (DOJ). 2008. *Federal Statutes Relevant in the Information Sharing Environment*. Washington, DC: DOJ.

———. 2006. *Legislative Analysis of the National Infrastructure Protection Act of 1996.* Washington, DC: DOJ.

Dycus, Stephen. 2010. "Congress's Role in Cyber Warfare." *Journal of National Security Law and Policy* 4: 153-169.

Dycus, Stephen, Arthur Berney, William Banks, and Peter Raven-Hansen. 2006. *National Security Law.* New York: Aspen.

"Electronic Communications Privacy Act of 1986," 8 *U.S.C.,* §§2511, 2516-18, 2515, and 2701-12.

Eskridge, William J., and Lauren E. Baer. 2008. "The Continuum of Deference: Supreme Court Treatment of Agency Statutory Interpretations of Chevron to Hamdan" *Georgetown Law Journal* 96: 1083-1226.

Falliere, Nicholas, Liam Murchu, and Eric Chien. 2011. *W32 Stuxnet Dossier.* Symantec. Accessed April 20, 2011. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

Federal Communications Commission (FCC). 2011. "Cyber Security and Communications." Accessed April 28, 2011. http://www.fcc.gov/pshs/techtopics/techtopics20.html.

———. 2009. "FCC Homeland Security Liaison Activities." Accessed April 10, 2011. http://www.fcc.gov/pshs/docs/liaison.pdf.

"Federal Information Security Management Act of 2002," 44 *U.S.C.,* §§3543, 3546, and 11331.

Fisher, Louis. 2007. "Invoking Inherent Powers: A Primer." *Presidential Studies Quarterly* 37: 1-22.

Goldsmith, Jack and John F. Manning. "The President's Completion Power." *The Yale Law Journal.* 115: 2280-2311

Gorman, Siobhan. 2009. "Cybersecurity Chief Resigns." *Wall Street Journal*, 7 March.

Government Accountability Office. 2010a. *Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Met*. Washington, DC: GAO.

———. 2010b. *United States Faces Challenges in Addressing Global Cyber Security and Governance*. Washington, DC: GAO.

———. 2008a. *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability*. Washington, DC: GAO.

———. 2008b. *Defense Production Act: Agencies Lack Policies and Guidance for Use of Key Authorities*. Washington, DC: GAO.

———. 2006. *The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information*. Washington, DC: GAO.

Gross, Michael Joseph. 2011. "A Declaration of Cyber War." *Vanity Fair*, April.

Hathaway, Melissa. 2011. *Briefing: Cyber Policy: A National Imperative*. Cambridge, MA: Belfer Center for Science and International Affairs, Harvard University.

———. 2010. *Briefing: Cybersecurity: The U.S. Legislative Agenda, Part II*. Cambridge, MA: Belfer Center for Science and International Affairs, Harvard University.

Herrera-Flanigan, Jessica. 2011. "Cybersecurity Ecosystem: The Future?" *Nextgov.com*, 24 March.

"Homeland Security Act of 2002," Public Law 107-296, Title II.

"Intelligence Authorization Act for Fiscal Year 2004," Public Law 108-177, Title III Section 316.

"Intelligence Reform and Terrorism Prevention Act of 2004," Public Law 108-458, Title I, Subtitle A Sec. 102A and Subtitle D.

Internet Security Alliance. 2010. *The Financial Management of Cyber Risk.* Arlington, VA: ISA/ANSI.

"John Warner National Defense Authorization Act for Fiscal Year 2007," Public Law 109-364.

Joint Chiefs of Staff. 2010. *Memorandum for Chiefs of the Military Services on Cyberspace Operations Lexicon*. Washington, DC: JCS.

Katyal, Neal K. 2006. "Hamdan v. Rumsfeld: The Legal Academy Goes to Practice." *Harvard Law Review.* 65:72-122

Kerr, Orin S. 2003."Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes." *New York University Law Review* 78: 1-9.

Kerr, Paul K., John Rollins, and Catherine Theohary. 2010. *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability*. Washington, DC: Congressional Research Service.

Kerry, Cameron F. 2011. "The Electronic Communications Privacy Act: Government Perspectives on Protecting Privacy in the Digital Age." Testimony before the Committee on the Judiciary, United States Senate. April6.

Koh, Harold. 2006. "Setting the World Right." *Yale Law Journal*: 2350-2379.

Lapointe, Adriane. 2010. *Oversight for Cybersecurity Activities*. Washington, DC: CSIS.

Lynn, William J. 2010 "Defending the Domain." *Foreign Affairs*: 97-108

Masters, Jonathan. 2011. "Council on Foreign Relations Backgrounder: Confronting the Cyber Threat." Accessed April 10, 2001. http://www.cfr.org/technology-and-foreign-policy/confronting-cyber-threat/p15577.

Merrill, Thomas W. 2002. "Agency Rules with the Force of Law: The Original Convention." *Harvard Law Review* 166: 467-592.

Moore, John N. and Robert F. Turner. 2005. *National Security Law, Second Edition.* Durham, NC: Carolina Academic

National Infrastructure Advisory Council (NIAC). 2007. *Convergence of Physical and Cyber Technologies.*

National Institute of Standards and Technology (NIST). 2010. *Special Publication 800-53: Recommended Security Controls for Federal Information Systems and Organizations (Amended).* Washington, DC: NIST.

"National Security Act of 1947," 50 *U.S.C.,* §15.

National Security Telecommunications Advisory Committee. 2009. *NSTAC Response to the White House Cyber Review Questions*. Washington, DC: NSTAC.

Nicholson, William C. 2005. *Homeland Security Law and Policy*. Springfield, IL: Charles C. Thomas Publishing.

Office of Management and Budget (OMB). 2010. *FY10 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management.* Washington, DC OMB.

Owens, William A., ed. 2009. *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Washington, DC: National Research Council.

Padilla v. Rumsfeld. 542 U.S. 426 (2004).

Rehnquist, William H. 1970. "The Constitutional Issues—Administration Position" *New York University Law Review* 45: 628-653.

Reinstein, Robert J. 2009. "The Limits of Executive Power." *American University Law Review* 59: 259-357.

Relyea, Harold C. 2007a. *National Emergency Powers*. Washington, DC: Congressional Research Service.

———. 2007b. *Presidential Directives: Background and Overview*. Washington, DC: Congressional Research Service.

———. 2005. *Terrorist Attacks and National Emergency Declarations*. Washington, DC: Congressional Research Service.

Rollins, John, and Anna Henning. 2009. *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations*. Washington, DC: Congressional Research Service.

Rosenzweig, Paul ed. 2009. *National Security Threats in Cyberspace Workshop*. American Bar Association Standing Committee on Law and National Security and the National Strategy Forum.

SANS Institute. 2009. "Twenty Critical Controls for Effective Cyber Defense: Consensus Audit." Accessed April 10, 2011. http://www.sans.org/critical-security-controls/interactive.php.

Skinner, Richard L. 2010. "Statement of Richard L. Skinner." Testimony before the Committee on Homeland Security, U.S. House of Representatives. Washington, DC: 16 June.

Stein, Glenn, and Basil J. Mitchell. 1990. *Administrative Law.* New York: Bender.

Sunstein, Cass R. 2005. "Administrative Law Goes to War." University of Chicago Law School Working Paper No. 90.

"Telecommunications Act of 1996," 47 *U.S.C.,* §§151 and 606.

"The Computer Security Act of 1987," Title 15 *U.S.C.,* §§271-278.

Theohary, Catherina. 2009. *Cybersecurity: Current Legislation, Executive Branch Initiatives, and Options for Congress*. Washington, DC: Congressional Research Service.

"Title III of the Omnibus Crime Control and Safe Streets Act," 5 *U.S.C.,* §5703.

Toomer, Jeffery A. 2003. *A Strategic View of Homeland Security: Relooking the Posse Comitatus Act and DoD's Role in Homeland Security.* Fort Leavenworth, KS: School of Advanced Military Studies, United States Army Command and General Staff College.

Tribe, Laurence. 1999. *American Constitutional Law.* New York: Thomson.

Tribe, Laurence, and Patrick O. Gudridge. 2006. "The Anti-Emergency Constitution." *Yale Law Review* 113: 1800-1870.

"USA PATRIOT Act as amended, 2008," Public Law 107-56.Title V Section 504, 505, 506 & Title VII.

U.S. Strategic Command. 2009. *Collaborating With the Private Sector*. Omaha, NE: USSTRATCOM.

"War Powers Resolution." 50 *U.S.C*. 33 §§1541-1543

The White House. 2011a. *Complete Cybersecurity Proposal*. Accessed May 12, 2011. http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/Law-Enforcement-Provisions-Related-to-Computer-Security-Full-Bill.pdf.

———. 2011b. *Complete Section by Section Analysis*. Accessed May 12, 2011. http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/Law-Enforcement-Provisions-Related-to-Computer-Security-Full-Bill-Section-by-Section-Analysis.pdf.

———. 2011c. *Presidential Policy Directive-8: National Preparedness.*

———. 2010. *National Strategies for Trusted Identities in Cyberspace*. Washington, DC: The White House.

———. 2009a. *Cyberspace Policy Review*. Washington, DC: The White House.

———.2009b. *NSPD 42: National Policy for the Security of National Security Telecommunications and Information Systems.*

———. 2008. *NSPD 51/HSPD-20: National Continuity Policy.*

———. 2007. *NSPD-54/HSPD-23: Cybersecurity Policy (unclassified summary).*

———. 2006. *The Federal Response to Hurricane Katrina: Lessons Learned*. Washington, DC: The White House.

———. 2003a. *HSPD-5: Management of Domestic Incidents.*

———. 2003b. *HSPD-7: Critical Infrastructure Identification, Prioritization, and Protection.*

———. 2003c. *HSPD-8: National Preparedness.*

———. 1989. *Executive Order 12472: Assignment of National Security and Emergency Preparedness Telecommunications Functions*.

———. 1982. *Executive Order 12382: President's National Security Telecommunications Advisory Committee.*

Whitley, Joe D., and Lynne K. Zusman, eds. 2009. *Homeland Security: Legal and Policy Issues.* Chicago, IL: American Bar Association.

Yoo, John C. 2001. *The Presidents Constitutional Authority to Conduct Military Operations Against Terrorists and Nations Supporting Them*. Washington, DC: DOJ.

Youngstown Sheet & Tube Co. v. Sawyer. 343 U.S. 579 (1952).

HOMELAND SECURITY STUDIES AND ANALYSIS INSTITUTE

An FFRDC operated by Analytic Services Inc. on behalf of DHS

2900 South Quincy Street • Suite 800 • Arlington, VA 22206-2233