Cyber Policy Solutions for Defense Mission Assurance in Critical Infrastructure

The Center for Infrastructure Protection and Homeland Security(CIP/HS)
George Mason University

Introduction

In a time of aging infrastructure and cyber threats at historic peaks, the concern of failure in the critical infrastructure that supports society touches every corner of the private and public sectors. The military is not immune to these concerns, and though defense installations implement extensive mission assurance measures to remain operational in the event of an attack, disaster, or other major disruption, significant interdependencies with civilian critical infrastructure remain in the daily operations of domestic defense facilities.

Day-to-day operations of most facilities still rely on the availability of community transportation, water, power, and communications infrastructure. Even where contingencies exist to cover shortfalls in these capabilities, the greatest longevity and efficiency in operations comes from ensuring the security and resilience of community resources.

The military is no stranger to engagement with the private sector. The Department of Defense (DoD) is the largest source of government contracts in the United States. In recent years, DoD has used the contracting process as a tool to enhance systems security for defense resources in the Defense Industrial Base, implementing security provisions to the Defense Federal Acquisition Regulation Supplement (DFARS).

However, these provisions remain relatively narrow in scope, addressing information security for controlled technical information and supply-chain security measures for national security systems. Existing regulations focus on manufacturing and research contractors in the Defense Industrial Base who engage directly with sensitive IT systems, which touch only the periphery of community infrastructure vulnerabilities. Furthermore, aside from direct intervention in operations, deterrence in the procurement system stems from legal liability under contract and tort, where damages are only applied after a breach has already occurred.

The legal framework for implementing effective security measures for these critical systems is in a constant state of development with solutions coming piecemeal from a wide assortment of actors. The tools that currently exist are utilized from a perspective that treats ad hoc implementation and *ex post facto* enforcement as adequate. These legal tools are

less cumbersome than prescriptive regulation and preventative measures, but the potential harm resulting from a massive disruption to the community power grid or transportation system is not easily remedied by monetary damages, especially when such a disruption bleeds into the operational effectiveness of a nearby defense facility.

For these reasons economic, policy, and legal tools must be implemented to provide DoD the ability to more directly influence maintenance and security of the critical infrastructure in communities surrounding defense facilities, especially in those lifeline sectors that most intrinsically support operations. In the following pages, we examine existing regulations and procedures in the contracting and acquisitions arena that could be adapted for contracts with local and regional asset operators and owners. We then examine other enabling measures that would grant DoD the necessary authority to more directly engage with both public- and private-sector entities responsible for the security and resilience of the critical infrastructure that feeds into these facilities.

Background

Current Critical Infrastructure Policy

While a full history of critical infrastructure (CI) governance in the United States is unnecessary here, a brief overview of current law and policy in the CI space would prove useful. The identification and distribution of CI sectors across federal agency jurisdictions has shifted several times over the past 25 years.[1] The current definition and classification of CI comes from the USA PATRIOT Act via Presidential Policy Directive 21 (PPD-21), issued by President Obama in 2013. Here, CI is defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[2]

Central policy in critical infrastructure protection (CIP) is communicated by DHS through the National Infrastructure Protection Plan (NIPP), now in its third edition, released in 2013.[3] In this document, CI taxonomy has evolved to a list of 16 sectors governed

---

[1] For an overview, see JOHN D. MOTEFF, CONG. RESEARCH SERV., RL30153, CRITICAL INFRASTRUCTURES: BACKGROUND, POLICY, AND IMPLEMENTATION (2015).

[2] The White House, *Critical Infrastructure Security and Resilience*, Presidential Policy Directive/PPD-21 (Washington, D.C., February 12, 2013), available at https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil, *citing* USA PATRIOT Act of 2001 § 1016(e), 42 U.S.C. § 5195c(e).

[3] United States Department of Homeland Security (DHS), *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: DHS, 2013).

by several sector specific federal agencies with the Department of Homeland Security (DHS) serving as the policy hub.[4] Of these sectors, four have been identified as "lifeline" sectors: energy, transportation, water, and communications.[5] Given the size and scope of these sectors, most are the purview of non-DHS offices in the federal government—the Department of Energy, Department of Transportation, and Environmental Protection Agency for energy, transportation, and water, respectively.[6]

In its latest iteration, the NIPP outlines several policy changes, most relevantly a shift from protection to security and resilience, greater emphasis on the interplay of cyber and physical threats, and more promotion of public-private partnerships. Cybersecurity, in this context, is not a sector, but rather a consideration ubiquitous to all sectors.

This paper will focus on the lifeline sectors, particularly energy, and related cyber concerns, especially threats of kinetic cyber attacks, or intrusions that result in physical harm to systems and assets.[7] Loss of power results in more immediate consequences for operations involving all manner of other equipment, resulting in cascading disruptions across other sectors. Furthermore, outside of the communications sector, emerging smart grid technology shows the greatest potential to develop into a ubiquitous data network connecting CI assets.[8] That said, we do not discount the possibility that other physical lifeline assets have received inadequate attention and that improved standards for these systems may prove beneficial.

Cybersecurity Law and Policy

The law of cybersecurity has evolved slowly out of a combination of existing laws covering seemingly unrelated areas of criminal, antitrust, communications, and information law, among other, and newer laws that have tried to adapt to ever-changing digital technology.[9] With the bulk of internet-connected assets in the hands of the private sector, cybersecurity policy has remained a primarily civilian domain. The notion of cyber warfare is a fairly recent development and remains a subject of speculation in current legal

---

[4] Ibid., 9.
[5] Ibid., 17.
[6] Ibid., 11.
[7] Scott D. Applegate, *The Dawn of Kinetic Cyber*, 5th Annual Conference on Cyber Conflict (Tallinn: NATO CCD COE Publications, 2013).
[8] See generally, "Smart Grid," United States Department of Energy, Office of Electricity Delivery & Energy Reliability, accessed July 24, 2015, http://energy.gov/oe/services/technology-development/smart-grid.
[9] See ERIC A. FISCHER, CONG. RESEARCH SERV., R42114, FEDERAL LAWS RELATING TO CYBERSECURITY: OVERVIEW AND DISCUSSION OF PROPOSED REVISIONS (2013).

discourse.[10] Even as these conversations and the potential for military involvement in cyberspace grow, civilian industry and law enforcement remain the principal actors in matters of cybersecurity. Such is the case even when agents of foreign nations are the threat.

For instance, in 2014 the Department of Justice (DoJ) charged five Chinese military hackers for cyber attacks targeting several major United States companies, resulting in the loss of billions of dollars over nearly a decade.[11] Analogous physical attacks against U.S. assets by military personnel of a foreign government could be treated as a justification for retaliatory military action. In the case of these breaches, the U.S. government took to the courts, treating the attacks as criminal, rather than military, acts despite their perpetration by military agents of a nation.

As this illustrates, the Department of Defense (DoD) does not currently exercise a robust role in cybersecurity outside of the military and Defense Industrial Base (DIB). Cybersecurity for civilian assets is governed by a mix of authorities scattered across multiple government agencies coordinated by DHS.[12] In this role, DHS and the sector-specific agencies responsible for CI perform two primary functions: (1) coordinating and developing policies for uniformity and efficiency of cyber operations across and within the federal government and (2) engaging the private sector to encourage information sharing, reporting, and security best practices.[13]

Efforts to implement Federal government standards have been more successful than similar efforts to standardize security for private-sector assets to date. Since 1987, the National Institute of Standards and Technology (NIST), an agency within the Department of Commerce, has been responsible for developing standards for federal computer systems.[14] In 2002, NIST gained new cybersecurity research responsibilities (shared with the National Science Foundation)[15] and, with the Office of Management and Budget, took a greater role in

---

[10] See, e.g., Matthew C. Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)," *Yale Journal of International Law* 36, no. 2 (Spring 2011) 421-459, available at http://www.yjil.org/print/volume-36-issue-2/cyber-attacks-and-the-use-of-force-back-to-the-future-of-article-24.

[11] Ellen Nakashima and William Wan, "U.S. Announces First Charges Against Foreign Country in Connection with Cyberspying," *Washington Post*, May 19, 2014, http://www.washingtonpost.com/world/national-security/us-to-announce-first-criminal-charges-against-foreign-country-for-cyberspying/2014/05/19/586c9992-df45-11e3-810f-764fe508b82d_story.html.

[12] White House, PPD-21.

[13] FISCHER, FEDERAL LAWS RELATING TO CYBERSECURITY 3-4.

[14] See Computer Security Act of 1987, Pub. L. No. 100-235, § 3, 101 Stat. 1724, 1724-25 (1988) (NIST was known as the National Bureau of Standards until 1988).

[15] Cyber Security Research and Development Act of 2002, Pub. L. No. 107-305, 116 Stat. 2367.

developing federal agency cybersecurity policies and standards.[16] More recently, Executive Order 13636 directed NIST to create a cyber risk management framework.[17] The first version of this document, hereafter referred to as "the Framework," was released in February 2014.[18]

Unlike more specific standards NIST has developed for government security practices, the Framework is a high-level overview of voluntary measures a firm can use to customize a security "profile" to the particular circumstances of the organization. A full discussion of the Framework is beyond the scope we address here. In brief, there is nothing prescriptive or specific in the Framework's guidance. Instead, the Framework recommends that companies develop "target profiles" as a guide for expansion and implementation of security measures, leaving specific measures to be determined by each firm.[19] This customization may encourage adoption by a greater number of operators but limits the Framework's utility as an enforceable standard.[20] In the absence of prescribed standards, strong economic forces are necessary to promote comprehensive security among the diverse and abundant asset across the private sector.

The cost associated with loss to and prevention of cyber crime is one such force. Research indicates these costs are growing steadily each year. The Ponemon Institute found in an international study of 257 companies in 2014 that the average annualized cost per company of cybersecurity was about $7.5 million, representing a global increase of about 10.4 percent over the previous year.[21] In the same study, Ponemon found that the sector with the highest annualized cost was the Energy and Utilities sector at about $13.18 million per company each year.[22] As an industry that serves nearly all consumers in the country, utilities are lucrative targets for malicious actors. Not only do utility companies possess large amounts of consumer financial data, they also support vital public services like hospitals, sanitation, water, traffic control, and many others. Disruptions in public utilities, especially

---

[16] Federal Information Security Management Act (FISMA), 44 U.S.C. § 3544(a)(1)(B)(directing compliance with standards created by NIST under 40 U.S.C. § 11331).
[17] Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. 11,739 (Feb. 19, 2015).
[18] *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0 (Washington, D.C.: NIST, 2014), available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.
[19] Ibid., 13-14.
[20] Robert Nichols, Susan Booth Cassidy, Anuj Vohra, Kayleigh Scalzo, and Catlin Meade, "Cybersecutiy for Government Contractors," *West Briefing Papers* no. 14-5 (April 2014), 12-13, available at https://www.cov.com/files/Publication/42df1e52-f857-4459-8e3b-41383ca6919f/Presentation/PublicationAttachment/313eea21-adca-4e00-8eac-561a6f0d15a6/Cybersecurity_for_Govt_Contractors.pdf.
[21] *2014 Global Report on the Cost of Cyber Crime* (Traverse City, MI: Ponemon Institute LLC, Oct. 2014), 1.
[22] Ibid., 9.

power, can cause cascading disruptions across various other sectors. In communities that contain or abut defense facilities, these cascading effects could lead to disruptions in military operational readiness.

This is especially true with the emergence of the Internet of Things (IoT). IoT refers to the trend toward greater networking and integration of all manner of common electronics, allowing data sharing and control functions through connected devices.[23] In the consumer space, this includes wirelessly controlled appliances, entertainment systems, and even lighting. In the industrial sense, the IoT concept can be found in newer supervisory control and data acquisition (SCADA) systems, among others.[24]

The security and resilience impacts of the IoT model are constantly evolving and provide a double-edged sword. On the one hand, greater use of IoT devices follows the general trend toward decentralization of control systems. As networking technology has progressed, SCADA systems have moved away from monolithic networks tied to central control locations towards ever more distributed control networks.[25] As the networks increase in size and individual nodes become more autonomous, the damage inflicted on a system by the destruction or disruption of a single device or node is reduced. At the extreme, each device could be designed so that the loss of even a significant portion of the networked devices would not fully disrupt the continued function of the remaining systems.

While this resilience marks a clear improvement, such a configuration also introduces vulnerabilities in the form of increasing numbers of potential access points for a malicious hacker.[26] Without regard to security, the efficiency of an IoT system results from the integration of more functions between various devices connected in the network. The greatest utility would come from persistent connectivity of the maximum number of assets to all available wireless-enabled control devices (i.e., computers, phones, tablets, etc.).

---

[23] Jacob Morgan, "A Simple Explanation of 'The Internet of Things,'" *Forbes*, May 13, 2014, http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/.

[24] See, e.g.,Christopher Mims, "How the 'Internet of Things' Is Turning Cities into Living Organisms," *Fast Company*, Dec. 2011, http://www.fastcompany.com/biomimicry/how-the-internet-of-things-is-turning-cities-into-organisms/; Allison Boccamazzo, "B-Scada Launches New IoT Initiative at ITEXPO 2015," *IoT Evolution*, Jan. 28, 2015, http://www.iotevolutionworld.com/m2m/articles/397213-b-scada-launches-new-iot-initiative-itexpo-2015.htm.

[25] See "SCADA History," Sandia National Laboratories, accessed July 21, 2015, http://energy.sandia.gov/energy/ssrei/gridmod/cyber-security-for-electric-infrastructure/scada-systems/program-overview/scada-history/.

[26] The increase in access points is only one prominent concern for rapidly developed IoT systems. For a brief summary, see Sanjay Sarma, "I Helped Invent the Internet of Things. Here's Why I'm Worried About How Secure It Is." *Politco The Agenda*, July 2015, http://www.politico.com/agenda/story/2015/06/internet-of-things-privacy-risks-security-000096.

In this scenario, each asset becomes a potential avenue for access to a core system that is capable of controlling functions and data in all other networked devices. A vulnerability in a networked lamp outside a home could give a hacker access to the home's security system, for example. The likelihood of such access has been exacerbated by the rapid technological development of IoT devices to meet market demand. Technical capabilities have advanced so quickly that manufacturers seeking to capitalize on new products ahead of competitors have sold devices without adequate security measures included.[27] HP found as recently as July 2014 that as many as 70 percent of the most common consumer IoT devices on the market contained security vulnerabilities, averaging 25 vulnerabilities per device.[28]

Even without such direct access, hackers already exploit vulnerabilities external to a targeted system, leaving key elements of network security in the hands of third parties. The recent Target breach serves as an example. The hackers behind the Target breach were able to gain access to the company's network through spear phishing e-mails sent to an HVAC company with credentials for the Target network. By obtaining legitimate credentials through an employee of this contractor, the hackers gained access to the internal network of Target. Through this vulnerability, the hackers were then able to access the company's point-of-sale system and steal millions of pieces of customer data.[29] This type of vulnerability through a third party expands further if the seemingly isolated system, such as an HVAC system, is integrated with a company's internal network.

While data theft remains a significant concern for both commerce and national security, inadequate attention has been given to the capability of remote hackers to disrupt or even physically damage industrial equipment through purely digital means, what some have referred to as kinetic cyber threats. Experts have hypothesized such threats for years, with nightmare scenarios including manipulation of GPS systems and flight control systems to cause vehicular crashes, disruption of industrial controls for inherently dangerous equipment, etc.[30] Only recently have such concerns been proven a reality.

The first confirmed case of a successful kinetic cyber attack came as the result of the Stuxnet worm. This malicious code acts in three phases: (1) it infiltrates Windows-based machines and replicates across networked devices, including USB storage devices, (2) it seeks

---

[27] "HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack," HP Press Release, July 29, 2014, http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676#.Va_O7vl3k2y.
[28] Ibid.
[29] Brian Krebs, "Target Hackers Broke in Via HVAC Company," *Krebs on Security*, Feb. 14, 2014, http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.
[30] Applegate, *The Dawn of Kinetic Cyber*.

out Siemens Step7 software, a Windows-based industrial control program, and (3) it then compromises the programmable logic controls of the system, allowing for both monitoring and manipulation of equipment.[31] Reports suggest that in 2010 Stuxnet successfully damaged centrifuges in some of the uranium enrichment facilities operated as part of Iran's nuclear program.[32] Other reports suggest that similar attacks have been attempted elsewhere, though without success.[33] Still others suggest precursors to Stuxnet were behind pipeline incidents in Turkey several years ago.[34]

More recently, the German government reported that an unidentified steel mill in Germany was the victim of a sophisticated spear-phishing attack that resulted in damage to the facility's equipment. The attacker reportedly first gained access to the plant's office network, eventually working through to the industrial control system. The attacks resulted in multiple failures, including an incident where a blast furnace was unable to be engaged in a controlled shutdown, resulting in "massive damage."[35] The report indicates that the attacker likely had sophisticated technical skills not only in IT security, but also extensive knowledge of technical control systems and production processes.[36]

These attacks show that there is an extant threat to physical infrastructure that relies on networked control systems. With the current trend toward greater integration of system components, the future promises increased opportunities for cyber attackers wishing to target critical infrastructure with kinetic cyber attacks. Unfortunately, many utilities have traditionally chosen to forego regular system patching and updates for industrial control systems to avoid service outages.[37] As a result, even as regulators move to address such

---

[31] David Kushner, "The Real Story of Stuxnet," *IEEE Spectrum*, Feb. 26, 2013, http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.
[32] "Hack Attack Causes 'Massive Damage' at Steel Works," *BBC*, Dec. 22, 2014, http://www.bbc.com/news/technology-30575104.
[33] Jeremy Hsu, "Stuxnet-style Virus Failed to Infiltrate North Korea's Nuclear Program," *IEEE Spectrum*, June 1, 2015, http://spectrum.ieee.org/riskfactor/telecom/security/nsa-stuxnetstyle-virus-failed-to-infiltrate-north-koreas-nuclear-program.
[34] "2008 Turkish Oil Pipeline Explosion May Have Been Stuxnet Precursor," *Homeland Security News Wire*, Dec. 17, 2014, http://www.homelandsecuritynewswire.com/dr20141217-2008-turkish-oil-pipeline-explosion-may-have-been-stuxnet-precursor.
[35] Kim Zetter, "A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever," *Wired*, Jan. 8, 2015, http://www.wired.com/2015/01/german-steel-mill-hack-destruction/.
[36] Bundesamt für Sicherheit in der Informationstechnik (BSI). *Die Lage der IT-Sicherheit in Deutschland 2014* (Bonn; BSI, 2014), 29, available at http://www.wired.com/wp-content/uploads/2015/01/Lagebericht2014.pdf.
[37] Lindsey Hale and Monta Elkings, "Simplifying the Patch Management Process," *The CIP Report* 14, no. 9 (June 2015), available at http://cip.gmu.edu/wp-content/uploads/2013/06/The-CIP-Report-June-2015-Energy-Sector.pdf.

deficiencies,[38] many control systems are now outdated at a time when network integration is becoming more widespread.

Defense Engagement with Infrastructure

In PPD-21, the Department of Defense is given responsibility for only one CI sector, the Defense Industrial Base (DIB).[39] This sector includes the production, design, and research industries that enable military operations, but explicitly excludes commercial infrastructure for the power, communications, water, and transportation sectors, who are fully under the jurisdiction of their respective sector-specific agencies.[40] Within the DIB, DoD has provided a number of tools to improve cybersecurity, such as the DIB Cybersecurity and Information Assurance (CS/IA) program, which provides a voluntary mechanism for the sharing of cyber threat information within the defense community.[41] The National Council of Information Sharing and Analysis Centers (ISACs) also maintains a DIB ISAC as a vehicle for sharing threat information in an all hazards approach, which includes cyber threats.[42] To date, outside of contracting regulations, these other cybersecurity efforts remain voluntary for sector stakeholders and inapplicable for non-DIB utilities that service defense facilities.[43]

DoD operates a distributed network of facilities and installations both domestically and overseas on which it relies to generate its capabilities. As with installations in the civilian sector, these assets depend on civilian infrastructure to operate. In turn, DoD fulfils most of its requirement for essential services such as energy, communications, and water through contracts with local providers. DoD facilities link to their surrounding networks and to national capabilities through civilian transportation systems across land, sea, and air. DoD procures these services on an as-needed basis through contracts of varying duration. Often these procurement decisions are made locally on an installation, guided by local- or service-level policy.

---

[38] See, e.g., Version 5 Critical Infrastructure Protection Reliability Standards, 78 Fed. Reg. 72756 (Dec. 3, 2013).
[39] White House, PPD-21.
[40] "Defense Industrial Base Sector," Department of Homeland Security, accessed June 17, 2015, http://www.dhs.gov/defense-industrial-base-sector.
[41] See DoD-DIB CS/IA Cyber Incident Reporting & Cyber Threat Information Sharing Portal, accessed July 22, 2015, http://dibnet.dod.mil/.
[42] See "Member ISACs," National Council of ISACs Website, accessed July 22, 2015, http://www.isaccouncil.org/memberisacs.html.
[43] This is not to say that ISACs and other information sharing tools do not exist for these firms, but rather that the defense community is not able to utilize these tools for the same kind of guidance and evaluation as it can for the DIB.

Monitoring these contract relationships and the performance of local service providers falls to installation- and service-level contract offices. In the case of lifeline services,[44] delivery will in many cases be limited to one or a few providers in the vicinity of the installation. Connection of these lifeline services to the installation requires coordination between the local service provider and installation logistics personnel. There are a host of local policies and procedures that are beyond the scope of this study for analysis, but all rest on the basic foundation of the authorities defined in this study. In this light, leaders must establish whether local personnel operate with sufficient authority to ensure that providers of lifeline services deliver with a level of security sufficient to safeguard DoD assets.

In addition, DoD assets must operate with a degree of mission assurance sufficient to fulfil defense requirements. Disruptions in lifeline sectors carry the potential to compromise mission assurance, so local installations must ensure that security measures used by critical infrastructure operators remain sufficient to avoid disruption or minimize the consequences of a disruption to services should one occur. Mission assurance requires DoD to have relationships with private-sector firms so as to ensure that security resources and practices are adequate in light of current trends of cyber vulnerabilities in civilian firms.

The U.S. Government Accountability Office has examined the degree to which DoD facilities rely on civil utilities, as well as the frequency and cost of disruptions in connected infrastructure.[45] The GAO Report on this topic found the DoD reported 180 power disruptions lasting 8 hours or longer in fiscal year 2013, resulting in an average cost of around $220,000 per day.[46] GAO suggests that current DoD reporting procedures for such disruptions are not comprehensive or entirely accurate and could be massively underreporting the frequency of such events.[47] In the past, these disruptions have been primarily the result of mechanical failures and extreme weather events, but GAO, citing the 2015 Defense Cyber Strategy,[48] notes that cyber threats will become a growing concern in the future.[49] As a result, DoD is developing guidelines for the cybersecurity of industrial control systems (ICS), due for implementation in 2018.[50] These guidelines will seek to address

---

[44] DHS, *NIPP 2013*, 17.
[45] U.S. Gov't Accountability Office, GAO-15-749, Defense Infrastructure: Improvements in DOD Reporting and Cybersecurity Implementation Needed to Enhance Utility Resilience Planning (2015), available at http://www.gao.gov/products/GAO-15-749.
[46] Ibid., 12.
[47] Ibid., 23-24.
[48] United States Department of Defense, *The Department of Defense Cyber Strategy* (Washington, D.C.: April 2015), available at http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.
[49] GAO-15-749 at 10.
[50] Ibid., 38-44.

vulnerabilities in DoD-operated ICS assets, but will not, under current plans, extend to external ICS that supports DoD facilities.

The threat to mission assurance posed by loss of service from community infrastructure has started a push for some facilities to seek independence from civilian services. This year Fort Knox became the first domestic defense facility to become completely self-reliant, allowing it to operate completely off the civilian power grid using completely renewable sources.[51] In addition to power independence, the installation is also capable of satisfying its own gas, water, and wastewater treatment needs. Though these measures are the culmination of decades of investment, the push for full self-sufficiency came after a 2009 ice storm left Fort Knox without power for almost a week, bringing operations to a halt and forcing soldiers to abandon their homes on the base.[52] If threats to civilian infrastructure near defense facilities continue to increase without adequate increases in security and resilience, Fort Knox could and should become a model for other facilities.[53]

The most recent strategic plans from DoD have included calls for increased utilization of reserve and National Guard forces to enhance cybersecurity capabilities within the active branches.[54] These forces are uniquely positioned to draw upon the professional and educational experiences provided by the civilian careers in which service members are engaged. Members of the Guard and reserve already working in high-tech jobs in information technology, finance, security, health, and defense firms possess a level of knowledge that would be expensive to replicate through training new recruits in the active branches.[55] These civilian careers also provide continuing education and training that would serve to supplement reservists' and Guardsmen's roles in a cyber task force. The Guard's flexible role as both a state and federal resource could also serve as a tool for harmonizing cyber policy at the state level. Through targeted recruitment, the Guard and reserve could increase the number of such skilled members moving forward ensuring a sustained pool of talent in the future.

---

[51] Capt. Jo Smoke, "Twenty Years of Energy Investments Pay Off for Fort Knox," U.S. Army, March 27, 2015, http://www.army.mil/article/145354/Twenty_years_of_energy_investments_pay_off_for_Fort_Knox/.
[52] Ibid.
[53] For other examples of military energy independence programs, see Kayla Matola, "Military's Shift Toward Renewable Energy," *The CIP Report* 14, no. 5 (June 2015), 17, available at http://cip.gmu.edu/wp-content/uploads/2013/06/The-CIP-Report-June-2015-Energy-Sector.pdf.
[54] Aliya Sternstein, "Pentagon to Recruit Thousands for Cybersecurity Reserve Force," *Defense One*, Apr. 16, 2015, http://www.defenseone.com/technology/2015/04/pentagon-recruit-thousands-cybersecurity-reserve-force/110407/.
[55] "NGAUS FY2015 Fact Sheet: Cyber Security and the National Guard," National Guard Association of the United States, accessed July 22, 2015, http://www.ngaus.org/sites/default/files/FY15%20Cyber%20Fact%20Sheet.pdf.

Legal Authority and Models

Legal tools in the areas of critical infrastructure protection and cybersecurity are numerous and scattered across various statutes, regulations, and executive orders. Taken broadly, these laws govern the authority and procedures for the federal government to contract with or directly regulate the private sector.

Current Executive and Legislative Cybersecurity Policy

With high-profile cyber attacks against various large companies in the United States increasing in frequency over recent years, cybersecurity has come to the forefront of national security policy.[56] Early in 2015, the President issued an executive order calling for measures to increase utilization of Information Sharing and Analysis Organizations (ISAOs) as defined in the Homeland Security Act of 2002.[57] The White House also released legislative and executive proposals to address gaps in current security policy.[58] These proposals identified information sharing and law enforcement as targets for legislative reform, and also drew attention to a 2014 report from DoD and GSA calling for improvement of cybersecurity through the federal procurement process.[59]

As it stands now, no major cybersecurity legislation has been enacted since 2002, with some smaller measures coming into effect, most of which address the security of federal systems.[60] Many proposals have been put forward in that time, with information sharing tools and standards topping the list of priorities for legislation facing the private sector. Several measures have been introduced in recent years to further enhance these efforts, including the reforms embodied in the Federal Information Security Modernization Act

---

[56] See, e.g., Robert K. Ackerman, "Destructive Cyber Attacks Increase in Frequency, Sophistication," *Signal* AFCEA, July 1, 2015, http://www.afcea.org/content/?q=Article-destructive-cyber-attacks-increase-frequency-sophistication.

[57] 6 U.S.C. § 131(5) (2015).

[58] "Securing Cyberspace–President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts," White House, Office of the Press Secretary, Jan. 13, 2015, https://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat.

[59] United States Department of Defense (DoD) and General Services Administration(GSA), *Improving Cybersecurity and Resilience through Acquisition* (Washington, D.C.: DoD/GSA, 2013), available at http://www.defense.gov/news/Improving-Cybersecurity-and-Resilience-Through-Acquisition.pdf.

[60] See FISCHER, FEDERAL LAWS RELATING TO CYBERSECURITY.

(FISMA) passed in 2014[61] and the Cybersecurity Information Sharing Act of 2015 (CISA) currently under consideration.[62]

Additional reforms enhance and refine NIST efforts by updating their research and standard-development authorities, including the establishment of statutory authority for the development of international cybersecurity technical standards and a federal cloud-computing strategy,[63] as well as to further formalize the central role of DHS in the coordination of federal information sharing by explicitly establishing the National Cybersecurity and Communications Integration Center (NCCIC).[64] With CISA and its equivalent House bills, Congress seeks to provide more tools for promoting information sharing in the private sector, most notably by providing a liability shield for participating firms. While Congress could certainly choose to go further in regulating the cybersecurity measures employed by the private sector, even those measures proposed in CISA have raised substantial controversy,[65] revealing the reality that direct regulation may simply be politically unfeasible.

Unlike the implicit lack of authority of civilian agencies, the authority for DoD to engage directly with the private sector is subject to explicit limitation. Perhaps the most explicit comes from the Posse Comitatus Act,[66] in which Congress placed limits on the ability of the military to act in a law enforcement context. The courts have drawn the line when interpreting this law at direct intervention in civilian law enforcement unless authorized by Congress.[67] Some argue this understanding limits the ability of defense personnel to act directly as law enforcement would in the prevention and response to malicious cyber attacks as well. As result of these limits, direct intervention in the security interests and operations of civilian infrastructure by the military typically follows a declaration of an emergency by some executive authority, usually at the state level.[68]

While law enforcement activity is broadly limited, other avenues for the military to influence private industry exist at the intersection of commerce and security. In certain

---

[61] Pub. L. No. 113-283, 128 Stat. 3073 (2014).
[62] S. 754, 114th Cong. (2015); see also Protecting Cyber Networks Act (PCNA), H.R. 1560, 114th Cong. (2015); National Cybersecurity Protection Advancement Act of 2015 (NCPAA), H.R. 1731, 114th Cong.
[63] Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274, 128 Stat. 2971, §§ 501-503.
[64] National Cybersecurity Protection Act of 2014, Pub. L. No. 113-282, 128 Stat. 3066, §3. DHS established the NCCIC in 2009 through administrative means.
[65] See, e.g., "Stop the Cybersecurity Information Sharing Bills," Electronic Frontier Foundation, accessed June 12, 2015, https://act.eff.org/action/stop-the-cybersecurity-information-sharing-bills.
[66] 18 U.S.C. §1385 (2015). More generally, *posse comitatus* refers to the ability of a county sheriff to gather citizens to aid in law enforcement, see Black's Law Dictionary (10th ed. 2014).
[67] FISCHER, FEDERAL LAWS RELATING TO CYBERSECURITY 22.
[68] See Ibid., 21-22.

instances where national security would be put at risk, the Secretary of Defense can demand that DoD be given top priority by private contractors, even to the detriment of existing customers, under the authority granted by the Defense Production Act.[69] This authority is similar in many ways to the intervention the executive often exercises in times of emergency or war. However, outside of such extraordinary circumstances, DoD is not empowered to directly engage in regulating or dictating the security of the civilian community, even in the proximity of defense facilities.

Because the general law enforcement powers of the military are so limited, discussions of DoD involvement in civilian cybersecurity usually focus on the adequacy of disaster response. The constitution and supporting legislation, such as the Stafford Act,[70] provide the authority and tools to permit the President to order military aid for civilian authorities in non-law enforcement roles in the event of an emergency. However, mission assurance and operational readiness for defense facilities are concerns that mitigation and recovery do not adequately address. The goals in these domains are security and prevention, areas that DoD cannot promote directly through enforcement or regulation in the private sector under the limitations of *posse comitatus*. For these reasons, DoD activity must be economic rather than prescriptive.

This remains essentially true for the National Guard and reserve, as well. As such, plans to recruit more cyber expertise in the Guard and reserve forces will face some of the same hurdles regarding direct intervention for the prevention of cyber attacks, namely that such forces would exist to "aid agencies during crises."[71] The contours of what such a crisis would look like are untested, but the legal authority for the use of the Guard and reserves in support of civil authorities is largely the same as the active forces, with some exceptions.[72] Legal authorization could presumably be part of a decision by the Secretary of Defense to activate Guard forces for "homeland defense activity."[73] With such activation, Guard forces could be used to protect infrastructure for up to 270 days.[74]

---

[69] See JARED T. BROWN AND DANIEL H. ELSE, R43118, THE DEFENSE PRODUCTION ACT OF 1950: HISTORY, AUTHORITIES, AND REAUTHORIZATION (2014).

[70] Robert T. Stafford Disaster Relief and Emergency Assistance Act, 42 U.S.C. 5121 et seq. (2015)(providing federal authority and funding for states that request aid from federal civil and military resources in an emergency).

[71] Sternstein, "Pentagon to Recruit Thousands for Cybersecurity Reserve Force."

[72] For example, 32 U.S.C. § 112 outlines the use of National Guard forces for drug interdiction.

[73] 32 U.S.C. § 901 (defined as "an activity undertaken for the military protection of the territory or domestic population of the United States, or of infrastructure or other assets of the United States determined by the Secretary of Defense as being critical to national security, from a threat or aggression against the United States").

[74] 32 U.S.C. § 904(b).

As a practical matter, long activations for full-time service would tend to diminish the benefits of such a program. The synergy DoD hopes to capture by utilizing the Guard for a cyber task force depends on the balance of military service with a civilian career that provides training and experience in a rapidly changing field. Long-term interruption of the civilian careers of Guardsmen in this context would, over time, diminish the exceptional capabilities DoD hopes to capture.

The legal barriers to this kind of use of the National Guard are murkier. Several issues exist. For one, policy on information sharing needs to be in place to avoid violating consumer privacy rights if the National Guard took an active role in monitoring the networks of privately owned critical infrastructure systems. Standards would also need to be set for any pre-emptive action such a force could take in monitoring or interdicting a privately-owned asset or network connected to a critical infrastructure system, including how such activity would relate to civilian law enforcement. At a certain level of activity, such actions could be such that interference with privately-owned networks creates a conflict with the owner's constitutional due process and property rights. Controls would need to be established to avoid such conflicts when possible.

These issues exceed the scope of this paper, but they illustrate that, in the current legal environment, a Guard-based cyber task force would not be a permanent, persistent solution to security for community infrastructure. As it stands, the strongest legal authority for the use of such a force would come in an emergency, which would likely be in the aftermath of an attack. Even if this force could be effectively used for prevention, long-term sustained use for securing privately-owned infrastructure would serve to diminish the efficacy of the force by cutting it off from one of its greatest resources, the experience provided by a civilian career.

Defense Acquisitions Regulation

Within these limitations, DoD has one incredibly powerful tool—the acquisitions process. With the largest discretionary budget in the federal government, DoD has a greater capability than any other agency to utilize regulation of government contracting to encourage improvement in security practices of private industry. In the 2013 fiscal year, DoD acquisitions made up roughly two-thirds of the total federal acquisitions portfolio, amounting to over $300 billion.[75] As a more specific example, DoD is the single largest consumer of energy in the world, with energy use at permanent installations amounting to

---

[75] Andrew Hunter, *U.S. Governement Contracting and the Industrial Base*, Statement before the U.S. House of Representatives Committee on Small Business (Feb. 12, 2015).

about $4 billion per year.[76] Regulations applying prescribed terms on cybersecurity in contracts under this umbrella have the potential to create massive economic incentives for improved security.

DoD acquisitions are regulated by the Defense Federal Acquisitions Regulation Supplement (DFARS), located in 48 C.F.R. § 201 et. seq. These regulations comprise the defense-specific portion of the Federal Acquisition Regulation (FAR) rules, which govern federal contracts as a whole. To date, only two rules in the DFARS directly address cybersecurity and risk management, and both came into effect on November 18, 2013.[77]

The first relates to supply-chain risk and provides a set of tools for DoD leadership to cut off business with contractors and subcontractors who pose a significant threat to operations.[78] More specifically, the Secretary of Defense and the secretaries of the respective military branches, in consultation with the Undersecretary of Defense Acquisitions, Technology, and Logistics (USD(AT&L)) and Chief Information Officer (CIO) can (1) exclude suppliers who fail to meet qualifications created under the authority of 10 USC §2319, (2) exclude sources that fail to achieve an acceptable rating on a risk evaluation, or (3) withhold consent for suppliers to subcontract with sources based on risk.[79] Decisions under this rule are not subject to review in any court.[80]

Though this authority seems broad, not all military suppliers are subject to these potential restrictions. While the mandatory contract clauses that enable this rule are required in every contract, these rules only apply to suppliers of components for use in national security systems (NSS), defined in 44 U.S.C. § 3552 as an information system used in intelligence, cryptography, command and control, weapons, or directly related systems, not including administrative or business systems. This narrow definition generally does not include utility contractors and many communications providers. This was an interim rule with a very limited comment period, indicating a belief that it addressed an urgent need of the department.

The second DFARS cyber rule addresses mandatory security measures to protect unclassified controlled technical information (UCTI) that is housed on or transits through

---

[76] Matola, "Military's Shift Toward Renewable Energy," 17.
[77] Before these rules were finalized, the Federal Acquisitions Regulation (FAR) Council proposed a similar, though far broader, rule applying to system security for all government contractors dealing with certain types of nonpublic information. The rule has yet to be finalized as of the writing of this paper. See 77 Fed. Reg. 51,496 (Aug. 24, 2012).
[78] Requirements Relating to Supply Chain Risk, 78 Fed. Reg. 69,268 (Nov. 18, 2013).
[79] Requirements for Information Relating to Supply Chain Risk, 48 C.F.R. §§ 239.7303-239.7305 (2013).
[80] 48 C.F.R. § 233.102 (2013).

contractor computer systems.[81] UCTI is defined as unclassified technical information, including both data and software, with military or space application that is subject to controls on access, use, reproduction, modification, etc. This information must be marked with one of the designations B through F described in DoD Instruction 5230.24, Distribution Statements on Technical Documents, indicating that the information has not been approved for public release.[82] This does not include information that is otherwise available publicly through other legal avenues.

For operators of systems that carry or hold UCTI, certain requirements may arise. First, contractors must implement a set of 51 security controls selected from those identified and described in NIST Special Publication (SP) 800-53. If a contractor fails to implement any of these controls, they may describe alternative measures in place that serve the same purpose or explain why a particular process or measure is not applicable to their system. If the contractor determines other security measures are necessary to maintain "adequate security,"[83] they must apply such measures.

Furthermore, the rule requires that contractors make detailed incident reports to DoD within 72 hours in the event of certain attacks that either directly affect UCTI or put it at risk.[84] Along with this reporting requirement, contractors must assist with DoD damage assessments following an attack. Both the security and reporting clauses must be included in any subcontracts entered by the contractor, including those with internet service providers and cloud services.[85]

Unlike the previous rule on supply chain risk, this rule went through a typical rulemaking process as described in the Administrative Procedures Act (APA).[86] In the original proposed rule, published in 2011, the new security requirements and reporting requirements were to apply to a broader category of unclassified DoD information, not merely technical information.[87] By narrowing the scope to technical information, this rule is much less likely to apply to utility contracts, although there are certain types of communications services contracts that could reasonably be expected to fall under the scope of this rule.

---

[81] Safeguarding Unclassified Controlled Technical Information, 78 Fed. Reg. 69,273 (Nov. 18, 2013).
[82] Safeguarding of Unclassified Controlled Technical Information, 48 C.F.R. § 252.204-7012(a) (definition of Controlled Technical Information).
[83] Defined in 48 C.F.R. 252.204-7012 as "protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information."
[84] 48 C.F.R. §252.204-7012(d).
[85] 78 Fed. Reg. at 69,274.
[86] See 5 U.S.C. § 553.
[87] Safeguarding Unclassified DoD Information, 76 Fed. Reg. 38,089 (June 29, 2011) (proposed rule).

The designation of sector-specific agencies at the federal level and the variety of state regulatory bodies for these services create further challenges for DoD engagement. Governance of the lifeline sectors spans myriad regulations at both the state and federal level. By their very definition, the public-facing nature of the services provided by these sectors subjects them to a greater degree of regulation than other commercial enterprises.[88] As an example, bulk power providers must comply with rules established both by the Federal Energy Regulatory Commission (FERC) and the responsible agencies of the states in which they operate. While cataloguing and discussing the rules of the various sector-specific regulators is beyond the scope of this paper, suffice it to say that some rules promulgated by these various agencies address cybersecurity to some degree. As a single example, FERC approved a new set of Critical Infrastructure Protection (CIP) Reliability Standards in 2013 that, once finalized, will serve as the primary source of cyber regulation for bulk electric systems at the federal level.[89] More recently, FERC has issued a notice of proposed rulemaking for an update to the current Physical Security Reliability Standard for bulk power assets.[90] Effective implementation of further measures by DoD through procurement or any other avenue would require communication, coordination, and collaboration with these various regulators to ensure harmonization of legal authority.

Analysis

Having examined the existing doctrines and legal tools that have been put forward in the form of executive initiatives, rules, and legislation, it comes time to look at the current situation that exists at the intersection of defense facilities and community infrastructure. Limiting our analysis to the most vital lifeline sectors of transportation, energy, water, and communications, all but transportation have a significant cyber component for community asset owners that could result in severe consequences for defense facilities in the event of a failure. Lapses in cybersecurity in the power grid, water system, or local internet or cellular provider systems could have cascading effects that would directly impact operations in area facilities, even if contingencies are provided. Disruptions to energy systems especially have the potential to hamper a multitude of other vital systems.

In economic terms, the equilibrium between the interests of the government in promoting cyber risk management standards and the cyber asset owner in minimizing cost will naturally tend to diverge, with the government favoring higher security standards. This

---

[88] 73B C.J.S. *Public Utilities* § 1 (2015).
[89] 78 Fed. Reg. 72756.
[90] Physical Security Reliability Standard, 79 Fed. Reg. 42734 (July 23, 2014).

divergence is the result of the principal-agent relationship between the contracting agency, here DoD, and its contractors.

Some essential tools for diminishing the gap between what the government considers to be optimal levels of investment in cybersecurity and contractor cost minimization goals are a natural product of the contracting process. In each case, the cost of improving system security will be passed along to the government to some degree, somewhat aligning the interests of the actors. In more competitive arenas, this cost alignment will be less pronounced as competitive bidding will cause contractors to absorb more of the expected cost to outbid competitors. This cost may be internalized either through increased investment outside the contract budget or by increased assumption of risk in the form of liability in the event of a breach.

Even though the infrastructure owners in the lifeline sectors discussed here generally do not face such competition, these industries are also heavily regulated and work with a large, powerful government agency in the DoD—two factors that translate to weaker bargaining power to pass security costs in contract bids. Furthermore, a typical scenario in which cost-reduction interests are aligned would involve principals with more flexibility to adjust expectations for security standards. For the DoD, working in an arena like national security based on a regulation like the DFARS UCTI rule, which cites a set of guidelines from NIST with both statutory and regulatory backing, there is very little flexibility for DoD to bring expectations into alignment with those of the contractors.

For these reasons, the government needs to take steps that bring the optimum security investment goals of contractors into alignment with the optimal standards. This can be accomplished in several ways, each with their accompanying costs and benefits. We start by examining the status quo, then examining each potential measure with the understanding that these measures could easily work in a number of combinations to achieve the best outcome.

The Status Quo

As it currently stands, the DFARS rules that address cyber risk management do not address the internal system security of contractors outside of those that house or transit UCTI. In most cases, such rules would not apply to critical infrastructure owners who contract to provide energy or water to defense facilities, though certain communications services, such as internet service providers (ISPs) would.[91]

---

[91] 78 Fed. Reg. at 69274 (noting that ISPs and cloud services qualify as subcontractors under the rule and would be expected to comply).

Absent greater legal authority, the government is limited to those remedies available for breach under contract law and tort. The most obvious consequence of reliance on these remedies is the delay in compensation that comes from any form of *ex post facto* enforcement action. While money damages obtained after a breach of contract are adequate for many types of business transactions, especially those more typical of the standard manufacturing and operational service functions, the catastrophic damages that security standards are meant to deter are not so easily addressed with monetary compensation after an attack. The risk management standards envisioned here and applied to cybersecurity in other contexts are designed to thwart malicious attacks by perpetrators who intend to maximize harm and who are often unreachable in court. These situations leave victims with the bill and, when security is found lacking, legal liability to other affected parties. In these contexts, prevention must be a top priority.

In fact, the circumstances in which similar malicious attacks would come from the critical manufacturing sector are already addressed by the recent interim rule on supply chain risk management discussed in the previous section.[92] This rule, which allows DoD officials to blacklist dangerous suppliers, shows a concern for the inadequacy of *post hoc* damages as a remedy for lapses in security that allow or facilitate a malicious attack.

Beyond the adequacy of remedies under a tort and contract law framework, the default rules of liability do not fully address the principal-agent problem natural to government contracts. Unless the government clearly defines the security standards to be followed by the contractor, the standard of care for security would fall into the subjective realm of the "reasonable person" standard.[93] While this reasonable level of security would certainly be informed by existing frameworks, there would be room for argument as to the reasonable standard of care the contractor needed to perform, and that standard of care would certainly not need to conform in any particular way to the NIST guidance that government agencies are now favoring.

This uncertainty that stems from the judicial process and the task of determining the proper level of care to avoid liability affects the cost calculations undertaken by the contractor when determining the optimal level of investment in security. At each level of investment, the probability of the contractor being found liable in the event of a breach would be a factor in determining the cost of the investment. This would follow a simple cost-benefit analysis.

---

[92] 48 C.F.R. § 239.7300 et. seq.

[93] See, generally, Restatement (Second) of Torts § 283 (1965); Dobbs' Law of Torts § 127 (2d ed., 2015).

As a simplified example, an investment of $300,000 in security improvements that would result in a ten percent (10%) reduction of the probability of being found negligent for a breach causing $1 million in damages would only have a value of $100,000. This probability, for the sake of avoiding complications, accounts for both the reduction in the likelihood of a successful attack and the reduced probability of a court finding the firm liable in a breach. Because the marginal savings is less than the cost of investment, the contractor would not undertake this investment. If the investment in question was necessary to meet some optimal level of security for the government, this would represent a discrepancy in the interests of the contracting parties and an inadequate level of security investment in the eyes of the government.

Setting a Standard

The obvious first step that has already been implemented across internal government systems is to set a clear standard for cyber risk management. For the most part, no standard exists for cybersecurity in the private sector, even for government contractors. This may be slowly changing with the increasing role of NIST beyond the development of internal federal standards, but the Framework discussed in the previous sections provides guidance that is voluntary and too general to be described as a serviceable "standard."

That being said, NIST has developed more precise guides that govern specific agency security practices within the broader scheme described in the Framework. For an example, we can look back to the current DFARS rules. NIST Special Publication (SP) 800-53, Revision 4 provides a selection of security and privacy controls that can be used in fulfilling some of the steps of the Framework's risk management process.[94] This particular guidance has been introduced as a formal standard for certain contractors through DFARS Rule 252.204-7012, which requires that contractors in control of systems that house or transit UCTI account for particular controls listed in NIST SP 800-53, Rev. 4.[95] Such adoption of current NIST standards intended for federal systems could be pursued in other contexts to push for heightened and more precise enforceable standards. Without such guidance, the Framework, though valuable as a mechanism for increasing risk management practices more generally, is too imprecise to be a true tool for standardization.

---

[94] Kelley Dempsey and Greg Witte, *Summary of NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations* (Washington, D.C.: NIST, 2014), available at http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800-53r4_summary.pdf.

[95] Joint Task Force Transformation Initiative, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53, Revision 4 (Washington, D.C.: U.S. Department of Commerce, 2013), available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

Assuming such standards are in place, reporting becomes a factor in the economic analysis of their implementation. In the case of the DFARS UCTI rule, this reporting occurs at the initiation of the contract and is enforceable through a mandatory clause in the acquisitions agreement.[96] In general, given the size and number of the contracts administered by DoD, this accounting will likely be the sole certification or audit for the majority of contractors. This fact, combined with the nature of many of the NIST guidelines, which are not matters of technical capabilities but rather of business practices like data retention and access control policies, indicates there is a significant risk that costly or cumbersome investments of effort and money to maintain operations at the level of the standards could result in a degradation of security over time absent further measures.

To illustrate using our previous example, if we start with the same $300,000 investment figure, we may examine the effects of a clear standard that is made mandatory under the contract. At the time the contract is made, an accounting must be delivered. Failure to account for the standards will result in a near certainty of contract breach, resulting in a potential spot on the government blacklist for high-risk contractors and loss of the current contract. It is not necessary to provide an exact value of the contract here, as we may assume that the contract value is adequate to warrant a $300,000 investment or the contractor would not have chosen to bid with knowledge of the requirements.

Having met the minimum standards under the contract, the possibility of liability still exists in the case of negligence. However, the reasonable person standard of care includes the existence of common practices as a factor,[97] and a court could use the NIST standards as a guide for the industry, reducing the likelihood of tort liability as long as the actors were, in fact, following prescribed practices. As it stands now, the Framework itself is not likely to serve as a standard of care for tort liability, though further adoption of the Framework and the use of its proposed "target profiles" could give rise to its use by plaintiff attorneys in the future.[98] Where more specific duties are identified, such as those in the DFARS UCTI rule, guidelines would be more likely to serve as a standard for tort liability. In light of these reductions in liability, the benefits of a shift from a position of near-certain liability to very likely non-liability are significant.

From here, we must be cognizant of the continuing cost of maintaining the practices that the NIST standards call for. If this $300,000 investment, or some substantial portion of it, is an annual cost rather than a one-time investment, a real possibility considering most

---

[96] 48 C.F.R. 252.204-7012.
[97] See, e.g., Cerretti v. Flint Hills Rural Elec. Co-op. Ass'n, 837 P.2d 330, 352-53 (Kan. 1992).
[98] Nichols, et al., "Cybersecutiy for Government Contractors," 12-13.

security practices are a matter of continuous monitoring and integration of new circumstances, the marginal benefit of the continuing investment would have to be measured for timeframes that follow the initial accounting by the government. The near certainty of contract breach in the first instance is a result of inspection by the government. The marginal benefit of the investment following this initial accounting would be the product of the anticipated loss from breach multiplied by the probability of an event that would call for another inspection of these practices, whether in the form of an audit or an attack that leads to a loss and subsequent enforcement action.

While it is difficult to say with any certainty what the probability of such an event would be, we can say with certainty that is lower than the near certainty of breach at the initial accounting. Unlike in the previous section, the likelihood of liability in the event of an attack is not the issue as the compliance with named standards informs the threshold for such determinations of liability. Instead, the probability that will affect costs is the likelihood of an audit or successful attack. If the chance of an audit is slight and the marginal increase in threat deterrence is believed to be inadequate to justify the cost, the contractor may choose to reduce investment in security after the initial accounting, opting for what would be considered an efficient breach of contract.

Because the uncertainty about the standard of care expected under the contract is reduced, the contractor's optimal level of investment in this scenario will invariably be higher than in a scenario without a contractual obligation to adhere to established standards. Over the life of the contract, without further measures, the maintained level of security will be below the government's optimal level, as represented by the named standards.

Other Liability Tools

Some additional cost-based mechanisms for adjusting the incentives that could be potential tools for addressing the principal-agent problem exist in the form of explicit liability shields, penalties tied to contract breach beyond damages, and periodic reporting requirements. These tools all have the ability to adjust the allocation of the costs of security to some degree.

Liability Shield

A shield to liability for malicious attacks enhances the previously described effect of an explicit standard on the probability of a contractor being found liable in the case of a breach. Whereas a requirement to meet specific standards would imply that those standards serve as the benchmark for a standard of care in judging negligence in the event of a breach, an explicit liability shield would provide certainty. In this scenario, the marginal benefit of maintaining standards would be increased somewhat even over that provided by simply

naming the standards as mandatory. As a matter of moral and legal principle, such a measure would also have the effect of removing implications of blame from the contractor for the malicious acts of a third party. The effect of this as an incentive for the compliance with a set standard is completely subjective and difficult, if not impossible, to quantify.

On its own, this effect may be minimal as an added incentive over simply mandating the standard, and a liability shield would have to be crafted to avoid providing too much protection for contractors. Should a liability shield be too broad, there is a certain danger of moral hazard. In other words, a contractor who might otherwise choose to invest in security beyond the minimum to meet the threshold to meet the mandatory standards would see a reduction in marginal benefit if the shield provides additional protection from liability. That said, these effects are the products of interests that cannot be understood in isolation. Unlike many manufacturers in the defense sector who subsist primarily on work with DoD, infrastructure owners in the community face liability to a wide range of customers, most of whom will be outside the federal government. A liability shield that is limited to federally contracted services will do nothing to reduce their liability to consumers or private-sector customers. These other customers reduce both the market power of DoD and the moral hazard effects of a liability shield.

Civil Penalties

Aside from adjusting the likelihood of liability for contractors, DoD could be given authority to set penalties for failures to maintain standards. Rather than adjusting the cost of security through shifting the probability of damages, pecuniary penalties would directly increase the cost of a failure to maintain standards by increasing the base liability of the contractor. To relate this to earlier examples, if a $300,000 investment is being considered to reduce the likelihood of liability by ten percent (10%) with damages estimated to be $1 million, a definite or estimated civil penalty of more than $2 million would increase the marginal benefit of the investment from $100,000 (10% of $1 million) to more than $300,000 (10% of $3 million), leading the contractor to make the investment. This example oversimplifies the equation in many respects; for instance, any variability or discretion by the body enforcing the penalty would reduce the anticipated cost of such a penalty. Despite this variability, the core concept remains sound.

Such a measure would require the setting of a mandatory standard as a prerequisite, and contract law's disfavor for penalties of this sort would mean that DoD would have to establish supporting authority for such a civil penalty either in existing law or through an

act of Congress.[99] Such measures would likely be unpopular with asset owners, and the need for political support to implement and maintain these penalties make such measures less appealing in many respects.

Periodic Reporting Requirements

The temporal aspects of the continuing investment in security that reduce the incentives for maintaining security standards after the initiation of a contract could be dissipated by requiring regular reports from contractors on the maintenance of security practices. These reports would increase the probability of a contractor being liable for a failure to meet mandatory standards for periods subsequent to the initial accounting described previously and used in current rules governing UCTI. If reports are frequent enough, there would be little to no opportunity for investment to lapse without a risk of breach.

Reporting requirements involve costs to both the principal and the agent similar to those of an audit. Reporting shifts much of the cost and burden of inspection and evaluation to the agent, leaving the principal with the cost of monitoring reports and pursuing enforcement for failures. The more frequent and thorough the reporting requirement, the greater the cost for all involved. While certain industrial actors are sensitive to the intrusions of such reporting requirements, infrastructure asset owners work in sectors that have historically been subject to heavy regulation and are less likely to find such requirements objectionable if the costs are reasonable.

These shields, penalties, and reporting requirements all presume a uniform standard, whether mandatory or voluntary, for maximum benefit. Furthermore, each is optimally used in combination with other measures because they each affect different elements of the cost-benefit calculation. All of these measures result in greater costs for all parties involved (in the form of moral hazard for shields and enforcement costs for penalties and reports). As a result, these measures, if utilized, must be the product of a careful balancing of interests.

Direct Regulation and Enforcement

Outside of market and contract-based measures, current and previous methods of direct action based on cybersecurity and risk management in other arenas offer options worth examining to deal with the system security of infrastructure asset owners. One such

---

[99] See Restatement (Second) of Contracts § 356 (1981); see also Priebe & Sons v. United States, 332 U.S. 407, 411 (1947)("It is customary, where Congress has not adopted a different standard, to apply to the construction of government contracts the principles of general contract law.").

option would be a rule allowing exclusion of certain contractors, similar to the current DFARS rule regarding supply chain risk management.[100] Another option would be for DoD personnel to have more authority to directly monitor and audit security measures for systems attached to community assets that feed into defense facilities.

Authority for defense officials to essentially blacklist infrastructure service providers would be potentially costly, if not impossible, to implement in most situations. Unlike the supply chain management rule and the situations it is designed to address, many of the infrastructure services that contractors provide to defense facilities are in markets subject to natural monopolies. Power and water utilities are among the most common natural monopolies in the U.S. economy, and telecommunications services that might be considered critical to defense facility mission assurance are going to be operated by a relatively small number of companies in any given area. This lack of competition makes it impossible to exclude contractors for existing facilities, bound geographically to a particular supplier. The only potential application of this type of criteria would be for new facilities, in which case a regulation is not strictly necessary. Rather utility security should simply be considered as one criterion in the selection process for facility locations.

Supplier exclusion could potentially be a useful tool for restricting the business practices of infrastructure owners in regards to subcontractors and suppliers for system equipment. While direct blacklisting of infrastructure owners cannot function in a monopolistic market, owners can be restricted from purchasing equipment or services from suppliers known to be a high risk. Such measures could be crafted to address risks from both malicious attacks via intentional system vulnerabilities introduced through tainted systems components or insider threats from subcontractors, as well as unintentional sources of increased risk from suppliers known to provide faulty equipment or deficient services.

Such measures could be effective, though one concern is the ability to enforce such measures when dealing with providers that have significant market power. DoD must have the authority and mechanisms to compel compliance, either directly or through the judicial process. Unlike current situations under which DoD can exclude suppliers, nearly all exclusions in the community infrastructure space would be exclusions of subcontractors, and canceling a contract with a monopolistic utility company that has engaged with a banned subcontractor will not be an option.

Alternatively, legal tools could be developed to permit DoD contracts to include mandatory clauses authorizing personnel to directly monitor and intervene in the security

---

[100] 48 C.F.R. § 239.7305.

practices relating to systems that could potentially compromise service continuity in critical community infrastructure. This option would forgo attempts to deal with incentives, with the consequence of significant costs to the government and contractors, not to mention ill will.

Without yet discussing the wisdom of such a system, such a process would present a number of conflicts requiring careful navigation. First, direct regulation responsibilities of critical infrastructure sectors are already assigned to various other executive agencies. For those sectors discussed here, the Department of Energy, through the FERC regulations discussed above, engages with power, the Federal Communications Commission regulates communication services, and the Environmental Protection Agency regulates water utilities. These federal regulations are further supplemented by regulations at the state level. Direct regulation of services in these sectors, even at the community level in the vicinity of defense facilities, would require DoD coordination and harmonization with the work of these agencies. Furthermore, some utilities are not operated as private companies. For these publically-owned companies, there are potential conflicts at the borders of federal and state legal authority that could make it difficult or impossible for DoD to directly regulate security. Finally, unlike contractors in competitive markets, utility companies usually provide services to large numbers of civilian customers with no efficient way to segregate systems servicing military and civilian customers. Such operations often run in geographic regions where there are no alternative sources of power. In effect, the military would have to assume significant authority over the direct operation of a civilian commercial enterprise. The questions and consequences raised by such practices in the legal and political arenas could end up being the most costly of all.

Ultimately, these kinds of direct intervention are not likely to be the most desirable for many reasons, only some of which were explored here. The practicality of such measures from both a political and economic standpoint is questionable at best. While such options could be explored in those scenarios where bases are serviced by facilities segregated from the civilian power grid, DoD would still incur significant costs by accepting responsibility for system security. In recent decades, the military has generally chosen to sell energy assets rather than upgrade or maintain them. This cost-reduction mindset is as strong as ever in the current fiscal environment.

Findings and Recommendations

Based on the above analysis, certain features of the current system become apparent. Lifeline infrastructure in the community is integrally tied to the mission assurance capabilities of domestic defense facilities. Despite this reliance on civilian infrastructure,

DoD has almost no role in determining the adequacy of current security for the networks that control and service power, water, and communications assets that feed into defense facilities in the United States. The status quo presents a significant risk to national defense that needs to be addressed. To this end, we recommend the following:

1) ***DoD should craft contracting practices and regulations that take cybersecurity standards into account when engaging with utilities.***

As explored above, the opportunities and authority for DoD to engage in direct intervention with the private sector are limited by the Posse Comitatus Act and regulation by other agencies. Under this limitation, the best short-term solution for DoD is to use the procurement and contracting process to create economic incentives for increased security. The large value of defense contracts and the economic benefits that feed into communities near these facilities provide strong motivation for utilities to be responsive to conditions in DoD contracts. By requiring greater reporting and providing the proper liability protection in contracts to utilities that implement adequate security measures, DoD can both encourage increased security by critical infrastructure that supports mission assurance and establish a more complete survey of the threat landscape.

2) ***Greater emphasis should be placed on crafting incentives that promote prevention of attacks instead of remediation of damages.***

The current cybersecurity and contracting fields rely too heavily on *ex post facto* actions for breach. As the system exists now, prevention and security are promoted by providing voluntary tools, while the primary incentives for embracing those tools remain the threats of loss in data breach or system damage and the liability to third parties that would follow. Consequences for failed security only come after an attack, usually in the form of tort and contract claims meant to reimburse losses. Such remedies are wholly inadequate in the realm of national security, where an attack can easily result in damages outside of the possibility of monetary remuneration, such as compromises of military operational readiness or even loss of life. More tools must be created, whether under existing authorities or by new statutes, to provide *ex ante* incentives for adoption of adequate security measures, whether in the form of liability shielding, civil fines, increased regulatory auditing, or other measures not explored here.

3) ***There must be more coordination and collaboration between responsible agencies at the federal, state, and local levels to ensure harmonization of efforts to raise security standards.***

The lifeline CI sectors include some of the most heavily regulated industries in the United States. These regulators span all levels of government and include several agencies at

the federal level. Energy companies, for example, are subject to regulations at the state level, as well as the rules of the Federal Energy Regulatory Commission. In some cases, these utilities are publically owned or heavily regulated at the municipal level. Even as a matter of policy, while DHS has oversight duties for all CI, PPD-21 places regulation of each of the lifeline sectors outside of DHS. Any measures to be pursued or implemented by DoD would have to be in harmony with the efforts and regulations of these core regulators. This requires effective communication of defense needs and coordination of efforts to create a legal framework that can achieve goals efficiently without placing a burden on asset owners that will further skew the market forces influencing their security investment decisions. To some extent, harmonization at the installation level could come through uniform policies for a National Guard-based cyber task force, though it is unclear if such efforts would influence the sector-specific regulations of civilian agencies responsible for community infrastructure.

4) ***The NIST Standards and Framework should explicitly address the threat of kinetic cyber attacks.***

To date, cyber attacks have largely sought to affect information either by theft or disruption. As a result, most standards and reports on cybersecurity focus on information security and the prevention of these kinds of attacks. For utilities connected to defense facilities, information theft or loss are not necessarily the primary dangers, and recent events have shown that the threat of physical damage or disruption to infrastructure assets as the result of a cyber intrusion is real. As NIST undertakes an evaluation and update of its current publications, it should examine the adequacy of current practices to address threats that target control systems for such assets and, if necessary, provide special guidance for protecting such systems against kinetic cyber attacks.

5) ***DoD should be prepared to further promote the removal of domestic defense facilities from community infrastructure in the long term.***

As Fort Knox and other cases have shown, the technology exists to remove defense facilities from reliance on elements of the public infrastructure. Such improvements come at a cost, and time will show whether the investments pay off. One thing is certain, removal of defense facilities from reliance on civil infrastructure reduces the need for DoD to engage directly with the security of community assets for the sake of mission assurance. The cost would be great, but segregation of defense facility energy, water, and communications systems from the civilian infrastructure before smart grids become common would alleviate the potential for a wider arena of threats that would emerge from a grid integrated with networked information systems.

Conclusion

Having explored several options for Defense involvement in and promotion of community infrastructure security at the nexus between the private sector and defense facilities, recent policy guidance and regulations have shown a preference for encouraging private-sector initiatives to improve cybersecurity measures across the board. Both by promoting the creation of ISAOs and pushing for higher standards and vigilance in contracting, the federal government has shown a preference for creating incentives to drive the market for better security.

For the Department of Defense, this requires more than the current focus on supply chain risk management and information security on national security systems. It also requires an approach to security that does not limit cybersecurity to concerns about protecting sensitive information. At the nexus of critical infrastructure in the community and domestic military installations, system security is about integrity and resilience, and the price of failure may be too high to be repaid through pecuniary damages.

In this environment, DoD needs to seek the necessary authority and generate the necessary regulations to create incentives for heightened security standards among private-sector operators that feed the lifelines of base operations. Models already exist for several options, and the NIST standards for federal systems already provide a potential model that can be put forward as a threshold for effective system security. The necessary steps that remain are to generate the market forces that lead service providers in the energy, water, and communications sectors to bring their systems up to these marks.