Strategy Research Project

Critical Infrastructure Protection: Cybersecurity Information Sharing and Public-Private Partnerships

by

Colonel Fritzgerald F. McNair
United States Army

United States Army War College
Class of 2014

REPORT DOCUMENTATION PAGE

Form Approved--OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
15-04-2014	STRATEGY RESEARCH PROJECT	

4. TITLE AND SUBTITLE
Critical Infrastructure Protection: Cybersecurity Information Sharing and Public-Private Partnerships

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Colonel Fritzgerald F. McNair
United States Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Captain James E. Boswell
Department of National Security and Strategy

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College, 122 Forbes Avenue, Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

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

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

13. SUPPLEMENTARY NOTES
Word Count: 7235

14. ABSTRACT

National infrastructure provides daily critical functions across diverse and complex sectors of a privately owned industrial base. Over the last decade, cyber threats against critical U.S. infrastructure have increased significantly. Presidential directives, legislative proposals, and GAO assessments all indicate that increased information sharing within public-private partnerships is integral to U.S. efforts in Critical Infrastructure Protection (CIP).

15. SUBJECT TERMS
Cyber, CIP, E.O. 13636, Improving CI, CNCI, NSPD-54

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(w/ area code)*
UU	UU	UU	UU	38	

USAWC STRATEGY RESEARCH PROJECT

Critical Infrastructure Protection: Cybersecurity Information Sharing and Public-Private Partnerships

by

Colonel Fritzgerald F. McNair
United States Army

Captain James E. Boswell
Department of National Security and Strategy
Project Adviser

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Abstract

Title:	Critical Infrastructure Protection: Cybersecurity Information Sharing and Public-Private Partnerships
Report Date:	15 April 2014
Page Count:	38
Word Count:	7235
Key Terms:	Cyber, CIP, E.O. 13636, Improving CI, CNCI, NSPD-54
Classification:	Unclassified

National infrastructure provides daily critical functions across diverse and complex sectors of a privately owned industrial base. Over the last decade, cyber threats against critical U.S. infrastructure have increased significantly. Presidential directives, legislative proposals, and GAO assessments all indicate that increased information sharing within public-private partnerships is integral to U.S. efforts in Critical Infrastructure Protection (CIP).

Critical Infrastructure Protection: Cybersecurity Information Sharing and Public-Private Partnerships

Eternal vigilance is the price we pay for liberty.

—Thomas Jefferson[1]

National infrastructure provides daily critical functions across diverse and complex sectors of a privately owned industrial base. Over the last decade, cyber threats against critical U.S. infrastructure have increased significantly and indications and warnings bode that the trend will continue in volume and severity.[2] The National Security Strategy (NSS) specifically cites protecting the nation's critical infrastructure from cyber attacks via increased public-private partnerships as vital to America's enduring interests since private industry owns 80-90% of critical infrastructure.[3] While the current NSS highlights cybersecurity as one of the nation's most serious national security concerns, all elements of national power play a role in safeguarding the cyber domain. The legislative branch also declared cybersecurity of critical infrastructure as a serious national security risk and both branches cite public-private partnerships and information sharing as integral to U.S. efforts to protect and secure critical infrastructure. The fundamental question embodied in Thomas Jefferson's admonition for today's strategist is how does the government protect a domain that the free market created and privately owns?

To address this question and the wicked problem of growing threats to America's cyber-reliant infrastructure, federal policy emphasizes the importance of public-private collaboration. The three principal stakeholders in national cybersecurity (executive interagency, legislature, and industry) conducted various efforts towards the strategic ends of institutionalizing cybersecurity best practices and increasing the volume and

quality of information sharing via the Department of Homeland Security's (DHS) National Infrastructure Protection Plan (NIPP). The Government Accountability Office (GAO) and DHS assessed numerous aspects of NIPP strategy implementation citing issues and risks due to ways and means not aligning with ends.[4] Over the same period, the DoD conducted cybersecurity-related pilot programs and projects via public-private partnerships. Initial DoD efforts faced challenges similar to NIPP efforts, but recent Army projects with multiple Defense Industrial Base (DIB) companies have successfully achieved objectives of increased cross-boundary information sharing (to include classified information), enterprise adoption of best practices, and increased congressional support. To fully implement improved information sharing, DHS, Congress, and private infrastructure owners can leverage available DoD best practices and DIB partnership models to achieve NIPP strategic ends. More optimal NIPP strategies and unified action will increase national security and reduce the risk of a catastrophic or "cyber 9/11" event horizon for Critical Infrastructure Protection.

Executive Branch Role in CIP

To delineate the DHS role in cybersecurity, President George W. Bush established the Comprehensive National Cybersecurity Initiative (CNCI) in a National Security Presidential Directive (NSPD-54) to provide national policy guidance to DHS for a national cybersecurity strategy. NSPD-54 outlined priorities for information sharing regarding cyber threats to Critical Infrastructure and Key Resources (CIKR). NSPD-54 also specifically mandated a minimum set of operational standards for government cyber networks and constituted the first-ever "whole of government" approach to cybersecurity protection.[5] In a "whole of government" approach, collaboration and information sharing are essential best practices for integrated teams who work "by, with,

and through (others)" such as interagency, regional, and multinational partners, alliances and institutions.[6] To facilitate such an approach, DHS established a national cybersecurity protection strategy in 2006 to include formation of government and private sector partnerships councils to collaborate on strategy implementation and execution. Cybersecurity councils are critical enablers of the cybersecurity protection mission since private industry owns the preponderance of infrastructure and has vested interest to secure privately owned networks against cyber threats. DHS also issued the National Infrastructure Protection Plan (NIPP), which provides the overarching strategy for integrating the nation's critical infrastructure public-private councils into a single national effort.

Under the NIPP, DHS develops the national strategy and the plan of action and milestones (POAM) covering the 17 different sectors of critical infrastructure. The NIPP serves as the strategic roadmap for the 17 sector councils to develop and maintain their sector-specific plans (SSPs) and annexes in accordance with the NIPP base plan.[7] The NIPP is therefore similar to a Combatant Commander's Theater Campaign Plan or an Assistant Secretary of State's Joint Regional Strategy with their respective supporting plans and annexes. DHS assesses individual SSPs to evaluate whether gaps exist in the protection of critical infrastructure at the national level, and if so, works with respective sectors to address them. In 2006, GAO made its initial report to Congress on U.S. Government (USG) progress in development, implementation, collaboration and execution of the NIPP with private sector stakeholders and their associated SSPs. GAO found two major deficiencies: 1) inadequate information sharing between USG and the private sector, and 2) inadequate government resources to execute the NIPP

across all sectors. Since 2006, the GAO has conducted numerous reviews of the NIPP program across all infrastructure sectors to determine progress toward objectives. DHS also internally reviews and reissues the NIPP every three years. Throughout the litany of internal and external assessments of NIPP program management, inadequate information sharing and inadequate government resources remain as recurring findings and deficiencies.[8] GAO reports specifically highlight how the ways and means of U.S. national strategy on cybersecurity protection do not balance with the desired ends.

Following the Bush administration CNCI efforts, President Barak Obama preserved and built upon NSPD-54 by reasserting that the "cyber threat is one of the most serious economic and national security challenges we face as a nation."[9] President Obama further declared that the government and country was ill-prepared to counter current cybersecurity threats and ordered a thorough review of federal policies to defend critical infrastructure and development of a more comprehensive approach to cybersecurity. Furthermore, in 2013 President Obama issued Executive Order (E.O.) 13636 titled "Improving Critical Infrastructure Cybersecurity" designed to strengthen U.S. policies and increase information sharing between the government and private sector in critical infrastructure protection. E.O. 13636 established a voluntary set of national cybersecurity standards, and among other things, directed the executive branch to increase the volume, timeliness and quality of cyber threat information sharing with private sector stakeholders to better prepare for, prevent, mitigate, and respond to cyber threats.[10] The strategic end states for the current US cybersecurity policy are: increased adoption of cybersecurity best practices and standards across all sectors and increased volume, timeliness, and quality of cyber threat information sharing.

Legislative Branch Role in CIP

Achieving cybersecurity strategic ends requires a comprehensive strategy to address the complex, long-term and evolving nature of digital threats. Protection of critical national infrastructure is therefore a collective responsibility that requires policies, strategies, and laws remain relevant to address current and emerging cyber threats—stakeholders must continually balance concepts, resources, objectives and risk. Congress is responsible to ensure government means are available to execute the ways of national cybersecurity strategy. Congress also has the power to incentivize private industry to allocate more industry resources to NIPP efforts, as well as, incentivize industry to increase their ways of sharing information via legislation that better protects industry's economic and legal interests and risks. Ultimately, increased congressional action enables sustained balance between ways and means, and increases the overall suitability of a national strategy to achieve desired ends. The 112th Congress made significant legislative efforts to address improving the collective national security of cyber infrastructure. However, despite a decade of legislative proposals, there remains no comprehensive legislation enacted on cybersecurity since the Federal Information Security Management Act (FISMA) of 2002. FISMA outlined an initial approach to the problem but only for the government sector.[11] Congressional support and oversight of national cybersecurity protection is essential to promote national strategies that are feasible, acceptable, and suitable.

Strategist's Role in CIP

The persistent challenges in protecting critical cybersecurity infrastructure across public-private sectors in terms of making the process a more cooperative and collaborative national enterprise, pose pressing questions for strategists: 1) how to

institutionalize more political support for cybersecurity resources, 2) how to increase the private sector's willingness to share sensitive (proprietary) information and resources, and 3) how to better translate infrastructure risks into costs that both Congress and private industry can buy into. To better balance the ends, ways, and means of national cybersecurity protection, strategists continually scan the environment for best practices to analyze and make necessary adjustments to operationalize strategy into effective plans. Typically, when addressing large-scale and highly complex problems involving innovative technologies, the USG turns to industry "best business practices" to formulate and adjust government strategic concepts or ways. However, in terms of information sharing (particularly of crisis or threat data) across diverse communities (e.g. "by, with and through" joint, interagency, intergovernmental, multinational, etc.) NIPP councils can leverage the proven "USG best practices" in information sharing within strategic partnerships to address the collective mission of protecting national infrastructure against cyber threats.

Industry Vantage Points on USG Role in CIP

Opposing views decry government solutions to cybersecurity since public initiatives by design presuppose private sector expenditure on national cybersecurity objectives (vice industry-driven objectives) and also run counter to industry's inclination to keep privately owned information private.[12] Opponents to federal cyber policies also contend that the very concept of national cybersecurity protection (against amorphous and ubiquitous threats) versus the obvious economic and social benefits of unregulated cyberspace is akin to fighting against the forces of nature or laws of physics. Opponents would argue that the "forces" of executive or legislative regulation, resources, and

political support cannot overcome the “centrifugal” forces of bureaucratic inertia and free-market capitalism whose objects tend to resist and push away from each other. Just as physics recognizes that “centrifugal” is not a “true force” but rather a resultant of inertia, supporters of government cyber initiatives can conversely argue that “centripetal” force (a real force) counteracts “centrifugal force” by preventing objects from flying off trajectory and moves them instead with uniform speed along a certain path. Industry supporters of a USG role in CIP therefore suggest that government resources, policies and laws are elemental forces that not only counteract inertia, but hold very large things together and help stakeholders better understand how they move.

Research Focus

Similar to the physics metaphor, this research analyzes how information sharing can act as a “centripetal force” (or a “centralizing” element of national power) in public-private partnerships to counteract organizational inertia and enable unified action in national cybersecurity strategy. Exploring the subject of national-level cybersecurity information sharing requires approaching the overall analysis based on its three elemental “forces” or stakeholder perspectives. Although all elements of national power play a role in safeguarding the cyber domain, this research focuses on the information element and specifically USG best practices in information sharing and strategic partnerships in the Department of Defense with DIB companies. Case studies of USG best practices in information sharing demonstrate proven strategies that yield increased volume, timeliness and quality of information, and what the private sector calls, actionable business intelligence (BI), which companies seek out for competitive advantage. Actionable BI is analogous to DoD’s decisive points in the Joint Operational Planning Process (JOPP), which when acted upon, give commanders a

competitive advantage. Studying proven USG best practices also offers potential options for DHS strategists to address the complex challenges of enabling unified action and implementing a unified campaign plan for the country against cyber attacks—a more comprehensive "whole of nation" versus a "whole of government" approach. This paper also lays out the analysis in three sections: 1) Defining the problem, 2) analyzing issues vis-à-vis objectives, and 3) exploring potential solutions.

Defining the Problem in CIP

The first step in answering strategy formulation questions about opening the aperture for protecting cybersecurity infrastructure to a comprehensive national view is to define this wicked problem from the three principal stakeholder perspectives—the executive interagency, the private sector, and the Congress to understand how each views the problem and how their respective concepts, resources and objectives relate to risk.

Executive Agency Perspective on the Problem

From an executive agency perspective, the overall NIPP and info-sharing strategy is a process requiring voluntary participation, robust commitment by industry and significant levels of trust within the interagency process and throughout the complex adaptive system of the NIPP public-private network. One GAO report surveyed both government and private sector council representatives to understand their respective definitions of problems facing NIPP strategy formulation and implementation. Although USG representatives acknowledged challenges in establishing and maintaining private sector cooperation, they defined the overarching problem in NIPP as private sector partners not meeting mutually agreed upon requirements. Under NSPD-54 and E.O. 13636, the executive branch cannot mandate industry participation, information sharing,

or compliance even in the case of mutually agreed upon cybersecurity standards and best practices. Presidential Directives (PDs) used by the executive branch to disseminate presidential decisions on matters of national security are forms of executive orders but neither PDs or E.O.s mandate or compel private companies to do anything that is not currently required under existing laws enacted by Congress.[13] This complexity creates a challenge for DHS similar to what Combatant Commanders (CCDRs) face in the interagency process. Combatant commanders are responsible for geographic regions and must share information, conduct planning and execute strategy collaboratively with interagency partners such as the Department of State to achieve strategic objectives directed by the national command authority. CCDRs develop Theater Campaign Plans (TCPs) with associated interagency roles and responsibilities codified in supporting plans and annexes, but CCDR's TCPs are essentially recommendations to interagency partners (such as Ambassadors) who do not answer to or have to comply with DoD recommendations. Interagency partners are not required to comply because civilian-led agencies operate under different authorities and pursuant to the U.S. constitutional paradigm of civilian control of the military.

Due to constitutional separation of powers and limitations of the commerce clause (particularly in cyberspace), public-private partnerships like the NIPP remain voluntary where trust is a critical enabler to sharing information and working collaboratively toward desired ends.[14] A 2010 GAO report highlights DHS reported challenges with private sector NIPP partners providing consistent levels of commitment and information. The GAO report specifically cites three categories of expected private sector services in support of the NIPP: 1) commitment to execute plans and

recommendations (such as best practices), 2) timely and actionable cyber threat information, and 3) permission to conduct vulnerability assessments. DHS government sector representatives rated multiple private sector council partners as moderately meeting standards in all three categories above. The report further noted DHS assessments across multiple sectors of private companies' unwillingness to share proprietary information despite the government's special protections and provisions such as sanitization processes. Additionally, government council representatives reported to GAO that private sector partners did not consistently keep the government informed about suspicious activities on private sector networks and not all private companies gave permission to conduct vulnerability assessments of their private networks—the NIPP stipulates both activities as mutually agreed upon best practices. Due to all factors bearing on the problem, USG representatives indicated that private partners did not consistently provide the ways to support strategic ends.[15]

Industry Perspective on the Problem

From an industry perspective, private sector partners defined the problem differently and reported that government partners did not meet their NIPP commitments by inconsistently providing: 1) timely and actionable cyber threat information, 2) security clearances, 3) dedicated resources and 4) necessary cost-to-benefit analyses that justify the additional risk commensurate with sharing additional proprietary information.

In the same GAO report referenced above, industry council representatives reported that government partners provided classified threat information, security clearances and technical/policy expertise 78%, 74%, and 38% of the time respectively, which all fell below agreed upon standards.[16] In terms of trust, private sector representatives pointed to the USG as the problem here as well. Private sector council

members highlighted a 2011 DHS/DoS pilot program intended to be a feeder program for the NIPP as an example of government trust and programmatic problems. The pilot featured DHS/DoD as co-leads for sharing classified cybersecurity threat data with Defense Industrial Base (Base) companies. In the two-year pilot program that DoD eventually transferred to DHS, both DoD and DHS openly reported that it took the USG nearly nine months to establish trust and information sharing mechanisms between interagency USG partners before including industry partners in the process.[17] Trust issues are overlying and recurring themes in NIPP council relations and multiple private infrastructure owners across reported a lack of trust in the government's ability to use and protect sensitive information (trade secrets).[18]

NIPP sector councils must also collaborate across state and local levels where industry cited inadequate government resources as a major factor bearing on problems here as well. Private partners reported inadequate security clearances for industry personnel to receive classified information at all levels. Additionally industry pointed out that DHS failed to provide requisite technical and policy experts and tools to support baseline information sharing. Industry partners attributed these problems to decreasing DHS budget levels of annual grants (means for improving collaboration capabilities at the state and local levels) that fell steadily "from $344 million (FY 2005), to half that total in FY 2006 and FY 2007, to under $49 million in FY 2008—highlighting the need for more elaborate risk assessment tools to inform resource allocation and priorities for cybersecurity expenditure."[19]

A final problem industry reported was DHS policy to maintain an "all-hazards" approach to protecting national CIKR across the wide array of potential infrastructure

targets. This broad USG approach featured no standardized schema or programmatic metrics to track and prioritize risks in terms of a cost-benefit analysis.[20] The private sector perspective on NIPP overall indicates insufficient USG ways and means to support the national cybersecurity strategy. This problem puts industry's ability to support its ends and the overall strategy at risk. In a period of declining federal resources for the foreseeable future, the NIPP focus on addressing "all" potential cyber hazards versus a prioritized approach (tiered based on the most at risk versus protecting all assets at the same levels) could discourage greater private sector investment, as well as, prevent greater congressional support until DHS defines a "good enough" cost-benefit methodology to better define risk.

Congressional Perspective on the Problem

Systematically defining the problem of national cybersecurity protection in terms of how much is good enough is also the fundamental problem from a Congressional or political perspective. Over the last decade, despite efforts by multiple sessions of Congress and more than 50 legislative proposals to address various aspects of cybersecurity either directly or indirectly, Congress has not enacted any overarching cybersecurity legislation since FISMA in 2002. The federal role in protection of privately held critical infrastructure remains a contentious issue of vigorous debate. Although there appears to be broad congressional agreement that growing cybersecurity risks to critical infrastructure require additional legislative action, there is considerable disagreement about how much, if any, additional federal regulation Congress wants to pursue.

In all legislative proposals since FISMA, Congress focused primarily on 10 issue areas and one key area was public-private information sharing. Congressional

cybersecurity proposals reflect broad consensus that barriers to public-private information sharing result from both federal and non-federal concerns about the risks of sharing classified data and industry proprietary information within and across sectors.[21] A key challenge for Congress in national cybersecurity protection is how to balance the need for sharing more timely and quality cybersecurity information with the need for protecting industry's economic and privacy interests since industry is the majority shareholder of national critical infrastructure. Right now, there is no clear or consistent congressional position on national cybersecurity strategy, which is arguably part of the problem.

Analysis of CIP Issues and Objectives

After defining the overlying set of problems from each stakeholder's perspective, the next step is analyzing each stakeholder's issues in light of their objectives for critical infrastructure protection.

Executive Branch Issues and Objectives

From and executive agency perspective, an overall NIPP objective is increased industry participation across all infrastructure sectors; however, industry's willingness to participate currently outstrips USG capacity to meet that demand. DHS established the NIPP in 2006, and after almost a decade of executive branch efforts to galvanize public-private partnerships, demand still exceeds supply. In 2011, a DIB cyber pilot (partnership between DoD, DIB IT companies, and DHS) objective was to expand sharing of classified threat data to approximately 8,000 eligible IT firms. However, DoD officials later revised their objective to 1,000 companies in the first year and to go after the remainder in following years. During 2011, DoD only signed up 17 of the eligible companies to participate.[22] DoD then transferred the DIB pilot to DHS in 2012 and DHS

objectives included expanding the total number of companies the USG shares classified data with, but DHS did not specify a numerical target. E.O. 13636 in 2013 supported DHS objectives and specifically authorized the Secretary of DHS to expand the number of companies the USG shares classified and unclassified cyber threat data with.[23] The total number of industry NIPP partners in 2012 when DHS took over the program was 962 and that number grew to 1,130 in 2013. To put NIPP overall industry participation in context, there were over 100,000 DIB companies supporting DoD in 2013.[24] The current number of NIPP private partners across all sectors compared to just the 8,000 eligible in the IT sector and those in the DIB in 2013 equals less than one percent of eligible companies. When one couples a roughly one percent industry participation rate (even after 3 years) with the aforementioned DHS challenge in meeting demand for processing security clearances (74% of the time), these altogether highlight an imbalance in USG means and ends. The degree of imbalance or risk is difficult to assess until DHS sets specific metrics for what level of industry commitment and resources across all sectors is "good enough" to protect infrastructure to a feasible, acceptable, and suitable degree.

Industry Issues and Objectives

From an industry perspective, NIPP private partners want the USG to provide more incentives and/or protections to increase participation, which amounts to more or less government regulation. Some companies want more government regulation to address legal, policy, and liability issues surrounding information sharing, otherwise they contend capability gaps in information sharing will persist. Industry proponents for more regulation believe E.O. 13636 is a step in the right direction, but comprehensive legislation is a critical requirement. Some IT sector industry partners, for example,

asserted that the huge increase of sophisticated cyber attacks after the Obama administration announced staffing of the E.O. (eight months before official release) was evidence that cyber attackers feared the E.O. would implement a nationally networked defensive strategy that would stop most known cyber attacks used in economic and military espionage. The IT sector expressed disappointment after official release of the E.O. because draft versions had outlined more meaningful standards for timely, reliable, and actionable situational awareness and resiliency, but the signed version did not. The IT sector blamed industry lobbyists for pressuring the White House to eliminate detailed standards that would have made cyber attacks less damaging and harder to launch.[25]

On the other hand, industry opponents of increased regulation believe E.O. 13636 is unnecessary and greater government regulation is counterproductive to overall NIPP objectives. Opponents instead believe the USG needs more and better incentives to influence private companies to spend more resources and assume more risk in sharing sensitive information to address ill-defined and obscure cybersecurity risks to infrastructure. Opponents further contend that imposing rigid USG cybersecurity requirements for evolving threats is imprudent since large government bureaucracies invariably lag in technological innovation. USG cyber initiatives amount to obsolete measures for real-time threats, effectively making systems less secure. Opponents instead advocate leveraging industry-driven best practices and standards to enable rapid information sharing, enhanced public private partnerships, and targeted investment to better target current and emerging threats.[26] Although both Industry opposing and supporting arguments above disagree on the amount and type of USG action needed in cybersecurity, both positions converge on the notion that more

meaningful USG action can help underwrite industry risk in balancing ends, ways, and means of NIPP strategy.

Congressional Issues and Objectives

From a Congressional perspective, many Members of Congress in recent years advocated an increased legislative role in underwriting industry risk in national cybersecurity to balance the ends, ways and means of NIPP strategy. Members on both sides of the aisle stood with Presidents Bush and Obama and declared that national cybersecurity was inadequate and that attacks to critical infrastructure posed a significant threat to national security. However, the over 50 legislative proposals and stated cybersecurity objectives fell short of consensus and amounted to unfunded mandates for NIPP national efforts since proposals did not carry the weight of law. The 112th Congress in particular passed several different bills including an update to the FISMA and the Cyber Intelligence and Sharing Protection Act (CISPA) in the House, but failed to pass the Senate. Senators wanted a more comprehensive bill that included FISMA and information sharing provisions, but Senators never codified their objectives into a bill. Some argue that failure of cybersecurity bills to pass the Senate resulted from opposition groups to increased federal regulation such as the U.S. Chamber of Commerce, other industry experts, think tanks, and interest groups.[27] Notwithstanding bureaucratic politics, Congress and DHS suffered from similar capacity issues in terms of failing to produce timely results, ineffective use of technical expertise, and applying limited resources to the problem.

For example, Congress has at least 86 different committees and subcommittees with some form of oversight of DHS. Such a diffuse committee and jurisdiction structure over critical infrastructure matters makes consensus difficult to obtain. Additionally, few

Members of Congress have detailed knowledge of homeland security and critical infrastructure protection issues despite being tasked to legislate on these matters, which only makes the problem worse. Consequently, cybersecurity oversight to date equates to an overly cumbersome, complex and inefficient system that makes substantive policy implementation and unified congressional action unattainable.[28] The current DHS committee structure prevents Congress from holistically understanding CIP challenges and addressing them appropriately through legislation. Congressional rhetoric versus action on cybersecurity therefore represents a "say-do" gap that degrades USG credibility and trust with industry stakeholders and falls short of supporting NIPP ways and means to achieve ends.

Exploring Potential Solutions

After analyzing each stakeholder's issues in light of stated objectives (how ways and means match ends) for protection of critical cybersecurity infrastructure, the next step is exploring potential solutions. Although the DHS-led NIPP program experienced challenges in achieving strategic ends of increased adoption of best practices and quality information sharing, other USG programs have proven success in similar endeavors. E.O. 13636 builds on the National Institute of Standards and Technology (NIST) developed cybersecurity technical standards and requires the DoD and the U.S. General Services Administration (GSA) to incorporate security standards in acquisition and contracting processes.[29] DoD arguably leads the federal sector in developing and managing enterprise level contracts that not only meet cybersecurity requirements, but also result in effective public-private partnerships that institutionalize both congressional and industry support in unprecedented manners—including increased information sharing.

Executive Agency Solutions

The Army's 2011 Cisco Enterprise Services Agreement (ESA) and associated public-private strategic partnership is a prominent example of a DoD best practice. Under the Army and Cisco ESA, timely information sharing, adoption of best practices, cost-benefit analyses, cybersecurity infrastructure, and congressional support all improved. From a USG perspective, improved Information sharing was the overarching objective and first order of business for establishing the Cisco ESA. For ESA governance, the Army created a program management framework that mirrored those used in the Defense Acquisition System (DAS) for USG program offices (PMOs), but the ESA version streamlined governance under a virtual organization overlaying existing USG structures (available means). The Army allowed Cisco partners access and participation in existing USG working groups and executive steering committees to embed collaboration, negotiations, and issue resolution mechanisms across all business areas up to the Army Chief Information Officer (CIO) and Cisco Chief Executive Officer (CEO) levels. The Army also created an unclassified and classified Integrated Database (IDB) that provided real-time asset visibility and business intelligence for 100% of army-owned Cisco software and hardware network infrastructure—a first-ever capability in the history of the Army. Establishing the first Cisco ESA and contract took two years of negotiations to develop and complete a public-private agreement capturing all technical, budgetary, and cost-benefit analyses that led to Cisco corporate leadership, DoD and congressional approvals. The ESA amounted to greater market share for Cisco while safeguarding their proprietary information and a $30 million annual savings for the Army.[30] In 2013, due to the numerous efficiencies and unprecedented cybersecurity infrastructure improvements

under the Cisco ESA, the DoD CIO directed the Defense Information Systems Agency (DISA) to leverage the ESA to establish a first-ever Joint ESA for all four military departments scheduled for contract award in 2014.[31]

Industry Solutions

DIB industry partners participate in Army ESAs at unprecedented levels. Increased participation in DHS NIPP councils is also a major objective of infrastructure industry partners. The Army ESA construct therefore provides a potential solution for infrastructure industry partners to address their issues in balancing ways, means and ends in the NIPP. The Cisco ESA framework specifically addresses NIPP industry concerns about timely and actionable information, increased USG technical expertise and security clearances for industry personnel. For information sharing, the IDB under the Cisco ESA is a powerful database and collaboration tool providing real-time analytics and metrics for managing the Army's network infrastructure. In 2011, Cisco software and hardware comprised 80% of the Army's network infrastructure and the Army managed its Cisco "enterprise" under 7000 disparate contracts decentralized across various Army commands. The Army CIO made the case that the Army could increase cybersecurity, operational effectiveness, and cost savings by consolidating authorities and funding for cybersecurity under the CIO and one umbrella contract. The IDB tool demonstrated for the first time Army capability for true "enterprise" asset visibility of unclassified and classified network infrastructure security, cost, and performance data. Accordingly, the IDB features a viable cost-benefit methodology for overall cybersecurity expenditure that benefits industry, DHS, and Congress. The IDB provides leading (versus traditional lagging) indicators for software and hardware life cycles so the Army can program in the budget process for replacement costs versus

end-of-year bulk purchases after product life cycle expirations—a common and inefficient DoD practice for buying commodity IT. The inefficient “end of year buy” practice contributes to market uncertainly for industry partners and constitutes a barrier to greater industry participation in potential business opportunities with the USG.

The IDB enables unprecedented information sharing on the classified side as well to meet industry demands for timely and actionable BI. There is a secret version of the IDB and Cisco provides cleared engineers to work in and support Army installations Network Enterprise Centers (NECs). The Army processes individual security clearances for Cisco personnel to work in Army facilities and also provides a centralized service for processing classified circuit and facility certification requests for Cisco facilities cleared to handle classified information. As a multinational corporation, Cisco Systems, Inc. supports a global Army network infrastructure, and is able to share, collaborate, and hold classified meetings (in person or virtual) between Army and Cisco working groups with unprecedented volume and efficiency due to the ESA. To establish and maintain trust in the ESA public-private partnership, the contract also requires quarterly program management reviews (PMRs) by Senior Cisco Vice President and staffs with the Army CIO staff to resolve issues and maintain strategic leader communications.[32] Cisco does not view PMRs or any USG requirements under the ESA as onerous or overly restrictive, and looks forward to increased business opportunities in DoD-level ESAs. Numerous other DIB companies also reached out to the Army CIO’s office to pursue ESA opportunities based on the Cisco ESA precedent.

Additionally, after public announcement of the Army Cisco ESA contract, Walmart representatives contacted Cisco to inquire about obtaining an enterprise

contractual agreement similar to the Army's. Walmart, a premiere and leading global business (outside the government infrastructure sector), expressing interest in adopting an ESA-like partnership is further evidence that Army ESA concepts, resources, ends, and risk management constitute a viable solution not just for the USG but for industry as well. The ESA model effectively enables balancing private sector needs for cybersecurity information and investment with their need to protect economic and privacy interests (i.e. resources versus risks). The ESA model is therefore ideal solution for industry in the NIPP public-private partnership in that it effectively addresses industry issues heretofore. In an ESA legally-binding contractual relationship, industry would be guaranteed the four primary requirements they reported as deficient in NIPP councils: timely and actionable cyber threat information, adequate security clearances and dedicated resources and the necessary cost-to-benefit analyses to justify cybersecurity costs to their shareholders. The Anti-Deficiency Act (ADA) specifically directs that all USG contracts with industry (that would include the above NIPP requirements by industry of the USG) must be fully funded (have congressional appropriation) before the USG can enter into a legally-binding contract as is the case with ESAs.[33] The ADA law under an ESA-like contract model for NIPP would guarantee DHS provides industry partners the solutions or means they require to support their roles in achieving NIPP ends in CIP. The ESA model provides industry a viable solution to meet information and resource requirements, and have the USG underwrite risks all guaranteed for a specified contractual period wherein industry also has systematic means to negotiate changes and updates as required. However, the ESA model only works effectively if Congress appropriates the resources required beforehand.

Congressional Solutions

Congress plays an instrumental role in supporting Army ESA projects and ultimately in balancing resources and risks for Army IT network infrastructure. Under the initial scope of the ESA model, the Army covered network hardware and software infrastructure under a single enterprise contract for the first time ever on a global scale. Next, the Army leveraged the ESA construct and awarded follow-on contracts for its major enterprise software license agreements (ELAs) awarding first-ever ELAs for Microsoft and Adobe in 2012—covered all software to include tactical and deployed users. These enterprise software mega-contracts consolidated all software product and service purchases and maintenance for the entire Army (all major commands and organizations where under Army executive agency) under single contracts with "IDB-like" database capabilities and real-time analytics.

Consequently, the Army realized 100 million dollars in annual cost savings in fiscal year 2012 due to total ELA and ESA contract efficiencies.[34] The Army's successful public-private partnerships and savings resulting from ESAs and ELAs not only influenced the DoD CIO to direct other services to follow suit, but also influenced congressional action due to the billions of dollars in projected annual savings over the contract periods. For example, Congress acted to support the ESA business model by directing the DoD to adopt similar best practices in the National Defense Authorization Act (NDAA) for fiscal year (FY) 2013 section 937 that directed:

> The Chief Information Officer of the Department of the Defense shall, in consultation with the chief information officers of the military departments and the Defense Agencies, issue a plan for the inventory of selected software licenses of the Department of Defense. The plan shall include the following: means by which the Department can achieve the greatest possible economies of scale and cost savings in the procurement, use, and optimization of selected software licenses.[35]

Congressional direction to DoD in Section 937 of the FY13 NDAA is a result of Army ESA/ELA unprecedented cost savings, and highly efficient public-private partnerships. The annual National Defense Authorization Act itself is a product four defense committees in Congress. Four committees manage the DoD budget effectively (withstanding periods of partisan gridlock) for a DoD enterprise that contains the largest employee workforce in the world and a budget of over 400 billion dollars.[36] The 86 committees and subcommittees that oversee DHS result in congressional action on cybersecurity that is disjointed, diffuse and ineffectual. If four principal committees manage oversight and budgets (to include allocating R&D funds for DIB projects) effectively for the scope and scale of the DoD, then fewer than 86 committees could streamline DHS oversight—to include cybersecurity research and development (R&D) funding for critical infrastructure protection. Even if congress cannot muster the consensus to enact NDAA-like legislation for DHS, there are other measures available to incentivize industry and help DHS balance ways and means to support a national cybersecurity strategy.

One private infrastructure company reinforces the notion that Congress has a role to plan in support of national cybersecurity infrastructure protection with the recommendation that, “Congress should prioritize federal funding for cybersecurity research and development, and should coordinate research activities between different participating agencies with industry input. Congress should also facilitate greater private investment in research more generally through the enactment of a permanent, simplified, R&D tax credit.”[37] The two recommendations above reflect exactly what Congress does annually to support DoD and the DIB. Congress provides billions of

dollars in research and development funding for DoD programs and projects with the DIB and Congress also provides tax credits to DIB companies. To maintain congressional support for critical DIB capabilities, DoD maintains a Manufacturing and Industrial Base Policy Office, the Office of the Chief Congressional Liaison (OCLL) and a host of other liaison and collaboration mechanisms at all levels to share information with Congress on DoD priorities and requirements. DoD views its DIB as a strategic asset and maintains multiple strategies to sustain its industrial base.[38] DHS could leverage DoD best practices of integrated information sharing (unclassified/classified), program management, and cost-benefit analyses with NIPP industry partners to facilitate more streamlined congressional support.

For example, as mentioned earlier, Congress has reduced DHS NIPP funding steadily since 2005. However, if DHS adopted a cost-benefit methodology similar to the ESA model that captures government and industry costs, leading BI indicators, efficiency goals, and resulting cost savings over multiple years, DHS could secure more NIPP resources or at least stave off significant future cuts. In 2011, the Secretary of Army tasked the CIO to return 1.5 billion dollars in IT efficiencies (total DoD target is 3.5 billion) by 2015 pursuant to the Office of Management and Budget (OMB) cost-cutting goals and presidential directed IT efficiencies in E.O. 13589.[39] The ESA/ELA cost savings contribute significantly toward meeting the CIO's goal and the Army CIO program received a budget surplus of 110 million dollars in FY12 to pursue six new ELA contracts.[40] Just as DoD sustains its DIB and the Army leads enterprise initiatives to sustain congressional support, DHS should consider similar strategies for preserving and expanding its infrastructure industrial base by institutionalizing congressional

support (means) for enhanced cybersecurity protection (ends) against growing threat vectors. Adopting DoD best practices in information sharing and public-private partnerships offers DHS proven strategies and mechanisms to not only increase congressional support, but also enable unified action across NIPP councils for a more comprehensive "whole of nation" approach to CIP.

Critics of ESA Model Solutions

Critics of the Army ESA model make two principal arguments that suggest ESA mega-contracts do not provide best value for the government and small businesses. First, critics assert that global ESA contracts limit competition by precluding small businesses (companies that gross less than $25.5 million annually and employee less than 150 people). Secondly, critics argue that ESAs give unfair advantage to incumbents with previous or existing Army contracts vice smaller companies that could potentially provide more innovative solutions. Both arguments underpin the Small Business Administration's (SBA) protest of the Army Cisco ESA contract lodged in 2012. The protest took a year to settle, but the SBA Office of Hearings and Appeals rendered its verdict in 2013. The SBA determined that the Army Cisco contract was legally awarded to Red River, Inc., a third party Cisco reseller and small business, under current code. However, SBA also ruled the small business contracting code that allowed the ESA needs to revision since in their opinion, no currently defined small business under the code could qualify for or satisfy the scope of products and services in global contracts that average nearly 100 million dollars in total value without substantial assistance (greater than 51% from the original equipment manufacturer—Cisco in this case).[41] Nonetheless, the Army continues to pursue and award ESA contracts in accordance with DoD and congressional mandates, but the SBA protest

raises valid critiques about overall USG competing objectives of increasing operational effectiveness, efficiency, and cost savings of contracts while also increasing small business participation (set asides) for large business sectors like the DIB and America's 17 infrastructure sectors. The requirements inherent in large-scale sectors may preclude participation by certain levels of small businesses without the in-house ways and means to provide global services or even national ones such as a resilient CIP. However, just like in the DIB, small businesses have options to team with larger companies or peers to tackle certain business opportunities and contracts. Also, there are two ESA features that militate against the SBA supposition in protesting that the Army Cisco ESA may not be a best value proposition. Under the Army ESA model, Army policy prohibits entering into contract negotiations with industry for any potential contract award unless two primary conditions are met: 1) industry proposals provide a cost-benefit analysis (CBA) for increased capability at less than or equal to current Army costs, and 2) the CIO submits an independent government cost estimate (with CBA) for the capability that the Army Budget Office also approves prior to negotiations.[42] Based the inherent features of the ESA, the model provides unparalleled economies of scale, best buying power and the overall best value to the government for critical network infrastructure capabilities. Ultimately, to address the valid concerns regarding policy mismatches that SBA raised in their protest, Congress and the SBA will have to prioritize USG contractual requirements and objectives for small business participation versus risks to national security and costs savings (particularly in the case of the DIB and infrastructure sectors) in light of declining federal budgets going forward.

Conclusion

National infrastructure provides daily critical functions across diverse and complex sectors of a privately owned industrial base. Over the last decade, cyber threats against critical U.S. infrastructure increased significantly and indications and warnings portend that the trend will continue in volume and severity. All elements or "forces" of national power play a part in safeguarding the cyber domain, and over the last decade, the executive and legislative branches declared cybersecurity of critical infrastructure as a serious national security risk. Both branches of government also cite public-private partnerships and information sharing as integral to U.S. efforts "by, with and through" industry partners to protect and secure critical infrastructure. The three principal stakeholders in cybersecurity conducted various efforts towards the strategic ends of institutionalizing cybersecurity best practices and increasing the volume and quality of information sharing via the DHS NIPP public-private partnership.

The GAO and DHS assessed NIPP strategy implementation and found systemic issues and risks due to ways and means not aligning with ends, despite presidential support over two administrations. Over the same period, DoD conducted cybersecurity-related pilot programs and projects via public-private partnerships. Initial DoD efforts faced challenges similar to NIPP efforts, but recent Army projects with multiple DIB companies successfully achieved objectives of increased cross-boundary information sharing (to include classified information), enterprise adoption of best practices, and increased congressional support. To fully implement improved information sharing, DHS, Congress, and private infrastructure owners can leverage DoD best practices and DIB partnership models to achieve NIPP strategic ends. More optimal NIPP strategies

and unified action will increase national security and reduce the risk of a catastrophic or "cyber 9/11" event horizon in Critical Infrastructure Protection.

Endnotes

[1] Thomas Jefferson, "Bennington," *Vermont Gazette* Online 1 (July 8, 1817): 2, http://www.monticello.org/site/jefferson/eternal-vigilance-price-liberty-quotation#footnote1_8928zcf (accessed December 15, 2013).

[2] U.S. Congress, Senate, Senate Select Committee on Intelligence, *Worldwide Threat Assessment of the US Intelligence Community: Statement for the Record by James R. Clapper, Director of National Intelligence*, 113th Cong., 1st sess., March 12, 2013, 1.

[3] Barack H. Obama, *National Security Strategy* (Washington, DC: The White House, October May 2010), 18, 19.

[4] Jena Baker McNeill and Richard Weitz, "How to Fix Homeland Security Critical-Infrastructure Protection Plans: A Guide for Congress," April 27, 2010, http://www.heritage.org/research/reports/2010/04/how-to-fix-homelandsecurity-critical-infrastructure-protection-plans-a-guide-for-congress (accessed January 11, 2014); U.S. Government Accountability Office, *Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed* (Washington, DC: U.S. Government Accountability Office, July 2010), 11-13.

[5] George W. Bush, *National Security and Homeland Security Presidential Directive-54* (Washington, DC: The White House, January 8, 2008), 5.

[6] U.S. Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States*, Joint Publication 1 (Washington, DC: U.S. Joint Chiefs of Staff, March 25, 2013), i.

[7] U.S. Department of Homeland Security, *National Infrastructure Protection Plan, Partnering to Enhance Protection and Resiliency* (Washington, DC: U.S. Department of Homeland Security, January 2009).

[8] McNeill and Weitz, "How to Fix Homeland Security Critical Infrastructure," 1-2; U.S. Government Accountability Office, *Critical Infrastructure Protection*,11-13.

[9] Office of the Press Secretary May 29, 2009 *Remarks by the President on Securing Our Nation's Cyber Infrastructure* http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

[10] Barack Obama, *The Comprehensive National Cybersecurity Initiative* (Washington, DC: The White House, January 2009), 5; U.S. President. Executive Order no. 13,636. Code of Federal Regulations. Title 3, § 4 (2013)

[11] Eric A. Fischer, *Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions* (Washington, DC: U.S. Library of Congress, Congressional Research Service, June 20, 2013), i.

[12] Chris C. Demchak, *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security* (Athens: University of Georgia Press, December 12, 2011), 175-181.

[13] John Contrubis, *Executive Orders and Proclamations, CRS Report for Congress #95-722A*, March 9, 1999, 1-2.

[14] Renee L. Giachino, "Commerce Clause in Cyberspace, Center for Individual Freedom," 2001
http://www.cfif.org/htdocs/legal_issues/legal_activities/policy_papers/commerceclause.html

[15] U.S. Government Accountability Office, *Critical Infrastructure Protection*, 11-13.

[16] Ibid., 14.

[17] Jared Serbu, "DoD Ready to Meet Pent up Demand for Cyber Threat Sharing Program," *DHS News, Federal News Radio,* May 15, 2012, http://www.federalnewsradio.com/473/2865055/DoD-ready-to-meet-pent-up-demand-for-cyber-threat-sharing-program (accessed January 10, 2014).

[18] U.S. Government Accountability Office, *Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics* (Washington, DC: U.S. Government Accountability Office, October 16, 2006), 21.

[19] McNeill and Weitz, "How to Fix Homeland Security Critical Infrastructure," 3.

[20] Ibid., 4.

[21] Fischer, *The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress* (Washington, DC: U.S. Library of Congress, Congressional Research Service, November 8, 2013), 7.

[22] Serbu, "DoD Ready to Meet Pent up Demand for Cyber Threat Sharing," 1.

[23] Jason Miller, "White House Issues Cyber Order, Giving NIST, DHS Lead Roles," *OMB News, Federal News Radio,* February 13, 2013, 3.

[24] U.S. Department of Homeland Security, *DHS Annual Report: Critical Infrastructure Partnership Advisory Council* (Washington, DC: U.S. Department of Homeland Security, 2013), http://www.dhs.gov/sites/default/files/publications/CIPAC_2013_annual_report.pdf (accessed January 15, 2014).

[25] Miller, "White House Issues Cyber Order," 2.

[26] "Securing the Network: Cybersecurity Recommendations for Critical Infrastructure and the Global Supply Chain," Telecommunications Industry Association White Paper http://tiaonline.org/policy/securing-network-cybersecurity-recommendations-critical-infrastructure-and-global-supply (accessed January 15, 2014).

[27] Miller, "White House Issues Cyber Order," 2.

[28] McNeill and Weitz, “How to Fix Homeland Security Critical Infrastructure,” 2, 8.

[29] Fischer, *Federal Laws Relating to Cybersecurity*, i.

[30] Fritz F. McNair, “Planning Program Budget Committee (PPBC) Review: Cisco Enterprise Service Agreement,” briefing slides with scripted commentary, Pentagon, DC, Office of the Chief Information Officer, April 17, 2013.

[31] Ibid., 2

[32] Ibid..

[33] *Antideficiency Act*, Public Law 258, 97th Cong., 2nd sess. (September 13, 1982), 923.

[34] McNair, “Planning Program Budget Committee (PPBC): Cisco ESA,” 3

[35] U.S. House. 112th Congress, 2nd Session. H.R. 4310, *An Act to Authorize Appropriations for Fiscal Year 2013 for Military Activities of the Department of Defense*, Washington, Government Printing Office, 2012.

[36] *U.S. Department of Defense Home Page*, http://www.defense.gov/about/dod101.aspx (accessed January 16, 2014).

[37] “Securing the Network: Cybersecurity Recommendations,” 4.

[38] Kris Osborn, “Pentagon Increases Efforts to Protect Defense Industrial Base,” *DoDBuzz Online Defense and Acquisition Journal,* September 12, 2013, http://www.dodbuzz.com/2013/09/12/pentagon-increases-efforts-to-protect-defense-industrial-base/ (accessed March 18, 2014).

[39] U.S. President. Executive Order no. 13,589. Code of Federal Regulations. Title 3, § 4 (2011); John Foley, “Army CIO Seeks $1.5B in IT Efficiencies,” *InformationWeek Online,* November 18, 2011, 1, http://www.informationweek.com/government/leadership/army-cio-seeks-$15b-in-it-efficiencies/d/d-id/1101427 (accessed March 18, 2014); John Foley, “Under Pressure, Pentagon Adopts New IT Strategy,” *InformationWeek Online*, November 16, 2011, 1, http://www.informationweek.com/government/leadership/under-pressure-pentagon-adopts-new-it-strategy/d/d-id/1101372 (accessed March 18, 2014).

[40] McNair, “Planning Program Budget Committee (PPBC): Cisco ESA,” 3.

[41] United States Small Business Administration Office of Hearings and Appeals “Size Appeal of Red River Computer Co., Inc.,” SBA No. SIZ-5512 (2013), 2.

[42]McNair, “Planning Program Budget Committee (PPBC): Cisco ESA,” 2.