CRITICAL INFRASTRUCTURE AND COMPUTER SECURITY:

Incentives and Policy in the Internet Era

Mike Specter, Webb Horn, and Chris Tam

Massachusetts Institute of Technology

EXECUTIVE SUMMARY

The United States relies on computer control systems, or SCADA systems, to handle fundamental utilities including the electric power grid, factories, water treatment plants, and medical facilities. Like any technology, these control systems are imperfect, but they are distinct from normal IT systems because they have the potential to cause enormous damage. Consequently, critical infrastructure computer systems have a direct impact on our national security.

Worse yet, the market in which SCADA systems are developed and utilized will naturally lead to insecure systems. The unique structure of the technology industry incentivizes the rapid creation of new technologies that typically include serious security vulnerabilities. Pressures on operators of critical infrastructure encourage them to adopt these new technologies, and the confluence of these incentives creates the potential for a national security disaster. It is therefore evident that regulation of the market is required.

Unfortunately, satisfactory regulation of critical SCADA systems does not currently exist. Beginning with the Patriot Act in 2001, the United States has sought to address the problem of insecure critical infrastructure computer systems through both legislative and industrial means. The existing efforts have not produced satisfactory results. In particular, they fail to continuously monitor the security of important systems, retain enforcement authority for their own regulations, incentivize the responsible disclosure of vulnerabilities, and strike an appropriate balance between a common set of IT best practices and sector-specific rules. We therefore call for the creation of new regulations that enforce higher standards of computer security for critical infrastructure.

We view the risks presented here as an immediate threat to national security that must be urgently addressed with a correspondingly aggressive regulatory solution. Our proposal includes four key recommendations:

1. Selection of an organizing agency with the power to enforce its policies and recommendations and the creation of a national "Red Team"[1] devoted to the continuous monitoring and assessment of critical infrastructure systems
2. A minimal common core of IT security requirements across all industries, with allowances for industry-specific policies

[1] Red Teams are a mechanism that organizations use to evaluate the security of their network. They consist of trained teams of attackers who play the role of malicious adversaries. Their ability to demonstrate security weaknesses in systems is well-documented and widespread (Acre & McGraw, 2004; see also Kramer, Carayon & Duggan, 2004). Given that the military and other government agencies already rely on them, we believe that they could play a strong role in defending critical infrastructure. See Section III for our specific policy proposals regarding red teaming.

3. A strong enforcement mechanism derived from financial penalties to ensure compliance with policies
4. Financial incentives for security researchers to find and responsibly disclose vulnerabilities

We believe that the only effective avenue to implementing these measures is by an act of Congress, and we urge policymakers to address our concerns responsibly, comprehensively, and quickly.

TABLE OF CONTENTS

EXECUTIVE SUMMARY 2
TABLE OF CONTENTS 4
INTRODUCTION 5
I. WHY REGULATION IS REQUIRED 7
A. Disastrous Consequences and Lack of Protections Indicate Need for Regulation 7
B. Current Incentives for Manufacturers Will Create Insecure SCADA Devices 8
C. SCADA System Users are Incentivized Against Security 8
D. Vulnerability Researchers are Incentivized to Make Attacking Easier 9
E. There is Need for Regulation for SCADA Systems 10
II. PREVIOUS POLICY EFFORTS 12
A. Recent legislation 13
1. CIPA and the Patriot Act Meet None of Our Recommendations 14
2. Cyber Intelligence Sharing and Protection Act Demonstrates Need for Civil Liberties Protections 15
3. SECURE IT Act Fails to Provide Regulation of Data Collection By Authoritative Agencies 16
4. The Cybersecurity Act of 2012 Addresses Key Points But Failed in Congress 16
B. Current Policy Initiatives 18
1. Executive Order 13636 and the Cybersecurity Framework Lack Enforcement Mechanisms 18
2. NERC-CIP is a Strong Policy Model for a Specific Industry 19
III. OUR POLICY PROPOSALS 21
A. Creation of an Organizing Agency and National Red Team for Continuous Monitoring 21
1. Funding is Scalable and Worthwhile 22
2. Civil Liberties Concerns are Valid and a Barrier to Entry 23
B. Strong Enforcement with Financial Penalties Increases Focus on Security 24
C. Incentivizing Responsible Disclosure Through Bug Bounties 24
D. Common Core of Security Requirements With Industry-Specific Policies 25
IV. CONCLUSION 26
V. APPENDIX 27
A. List of Commonly Used SCADA System Manufacturers 27
B. Other Miscellaneous Regulations 27
VI. BIBLIOGRAPHY 29

INTRODUCTION

In June 1982, NORAD detected an unexplained explosion measuring three kilotons in rural Siberia. Strangely, rather than being shocked, the White House National Security Staff was pleased. This explosion was caused by a CIA espionage operation in which the US sold the USSR flawed computer chips and software with the intent of damaging the trans-Siberian gas pipeline. This event, known as the Farewell Dossier, served as a lesson on economic espionage for the USSR and demonstrated an increasing global reliance on fragile computer-controlled critical infrastructure.[2] Despite this, the US has become much more reliant on such systems even though such attacks continue to this day. In fact, according to the US Government's Industrial Control Systems Computer Emergency and Response Team (ICS-CERT), an agency that deals directly with such systems in the US, critical systems at two power plants in the US were recently infected with malware.[3]

The Critical Infrastructure Protection Act of 2001 provides an important definition of the term "critical infrastructure":

> "...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."

In this paper, we focus on a subset of the infrastructure identified in Congress' definition—that is, we restrict our attention to infrastructure whose security is vulnerable to or compromised by threats to their computer systems.

Many of the everyday services that Americans take for granted—transportation, medical care, electricity, access to water and the Internet, etc.—are run by automated computer systems, leaving them open to the possibility of attack. Should one of these vulnerable systems be compromised, it could mean inconvenience, economic damage, and even loss of life.

In this paper, we argue that the unregulated tendency for all actors in the market for the computer systems that control critical infrastructure—known as Supervisory, Control, and Data Acquisition (SCADA) systems—is to remain insecure. In other words, we show that computer control system users and manufacturers are incentivized to leave their systems open to attack, and therefore require regulation. Our proposed regulation for SCADA systems that control critical infrastructure contains four key pillars: (1) the creation of a technical team devoted to continuously monitoring SCADA systems, (2) a minimal common core of IT security requirements across all industries, with allowances for industry-specific policies to fit our multi-stakeholder model, (3) a strong enforcement mechanism derived from financial penalties to ensure compliance with policies, and (4) financial

[2] William Safire. (2004, February 2). The Farewell Dossier. *New York Times*. Retrieved from http://www.nytimes.com/2004/02/02/opinion/the-farewell-dossier.html

[3] Industrial Control Systems Cyber Emergency Response Team. (2012). MALWARE INFECTIONS IN THE CONTROL ENVIRONMENT. *ICS-CERT Monitor*, (October/November/December 2012), 1–15.

incentives for security researchers to find and responsibly disclose vulnerabilities.

This paper is divided into three parts. Section I describes why the existence of SCADA vulnerabilities are a systemic issue caused by the free market, and it justifies why regulation is required. Section II reviews the shortcomings of current relevant legislation and regulations with regard to our policy suggestions, and provides an analysis of the benefits and criticisms of recent efforts. Finally, Section III justifies the comprehensive policies listed above, leveraging the information gathered in the first two sections. In sum, the purpose of this paper is to explain the SCADA system critical infrastructure problem, to understand the prior work with regard to regulation of the issue, and to formulate a set of goals and procedures that will effectively defend computer-controlled critical infrastructure.

I. WHY REGULATION IS REQUIRED

Threats to SCADA systems are real and documented. The natural tendencies of the market, left unchecked, will produce vulnerable critical infrastructure, and the dangers of SCADA system failures are too great to ignore. Although the example of the Farewell Dossier is dramatic, compromised SCADA systems can bring down hospitals, trap passengers in subways, redirect raw sewage into the water system, or disconnect the electric grid for entire cities.[4] In short, these are systems that can cause loss of life and must be protected accordingly.

A common critique of any government intervention in the market is that regulation without purpose can stifle innovation and disrupt the market by putting undue pressure on the natural tendency of businesses to find efficiency. This section presents an argument for why secure SCADA systems will not naturally occur in the free market, why the impact of the damage caused could be catastrophic, and that regulation is therefore necessary.

A. Disastrous Consequences and Lack of Protections Indicate Need for Regulation

Utilities represent a unique target for attackers because they can be targeted remotely using techniques that can make it difficult to identify attackers,[5] and because the effects of an attack on SCADA systems could be disastrous. SCADA systems are a class of control software that are commonly used to monitor and maintain utilities such as power, chemical, and sewage systems, as well as unique utilities such as uranium processing facilities, medical facilities, and various transportation systems.[6]

Counterintuitively, the impactfulness and risk associated with SCADA security breaches is not reflected in the current design of technical protection mechanisms. According to one study, "most devices appear to be highly vulnerable to even minor attacks and have no authentication/authorization mechanisms to prevent rogue control." For example, the protocol over which SCADA systems operate, modbus, has no option for authentication, so any actor on the internal network of a SCADA system can execute arbitrary commands.[7] So, if they are so important, why are these systems being left unprotected?

In order to understand this phenomenon, it is useful to individually analyze each actor in the

---

[4] Graham, R., & Maynor, D. (2006, January). *SCADA Security and Terrorism: We're Not Crying Wolf!* Presented at the Blackhat Security Conference, Washington, DC, USA. Retrieved from http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf

[5] Clark, D. D., & Landau, S. (2011). Untangling attribution. *Harv. Nat'l Sec. J.*, *2*, 323.

[6] Daneels, A., & Salter, W. (1999). What is SCADA. In *International Conference on Accelerator and Large Experimental Physics Control Systems* (pp. 339–343). Retrieved from https://accelconf.web.cern.ch/accelconf/ica99/papers/mc1i01.pdf

[7] Byres, E., & Lowe, J. (2004). The myths and facts behind cyber security risks for industrial control systems. In *Proceedings of the VDE Kongress* (Vol. 116). Retrieved from http://nealsystems.com/downloads/Myths%20and%20Facts%20for%20Control%20System%20Cyber-security.pdf

SCADA market. There are three discrete actors to consider: the manufacturers of SCADA systems; users of SCADA systems; and those that can discover vulnerabilities in SCADA systems. Below is a discussion of each of these actors, their incentives, and how these incentives yield insecurity.

B. Current Incentives for Manufacturers Will Create Insecure SCADA Devices

Comprehending why manufacturers will not naturally develop their systems with security in mind requires an understanding of the systems themselves. Complexity is part of the problem; there are numerous parts that go into the development of a SCADA system. A system's Human Machine Interface (HMI) warns a user of failures, and provides an operator with an interface to control the system.[8] HMI software typically runs on a commodity operating system and communicates with the SCADA hardware itself over the modbus protocol. SCADA hardware can be generally thought of as a remote, proprietary, real-time computer that performs physical actions and provides feedback to the HMI.[9] HMI software can be written either in-house by the utilities provider, or via drag-and-drop HMI software toolsets. Consequently, SCADA hardware manufacturers, user operating system developers, and HMI software authors share common pressures: each acts remarkably similar to a normal software or hardware firm.

When dealing with the IT industry, it is important to remember that the economic rewards of vendor lock-in and other first-to-market benefits trump the negative results of insecure software. Ross Anderson, Cambridge University professor of Computer Science and chair of the Workshop on Economics of Information Security, writes that in the commercial software market, the attitude of " we'll ship it on Tuesday and get it right by version 3… is perfectly rational behaviour in many markets where network economics apply."[10] He goes on to describe why such a situation would arise: software security is not incentivised by the market because normal buyers of software are unable to judge the security of that software and therefore decide which system to purchase based on other, more user-visible, aspects. The manufacturer is therefore unlikely to develop hardware and software with security in mind, resulting in an incredibly low bar for attackers.

C. SCADA System Users are Incentivized Against Security

Not only is there little incentive for SCADA operators to secure their systems, there is actually a large negative incentive to applying IT security standards to their networks. Although the consequences of a potential failure would seem to provide an incentive for users of SCADA systems to defend against vulnerabilities, our analysis of common uses of SCADA systems demonstrates this to be untrue.

Utilities tend to use these systems in large, dispersed, networked environments in which it is

---

[8] Graham, R., & Maynor, D. (2006, January). *SCADA Security and Terrorism: We're Not Crying Wolf!* Presented at the Blackhat Security Conference, Washington, DC, USA. Retrieved from http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf

[9] Allen Bradley. (n.d.). What is a PLC? *Ladder Logic*. Retrieved from http://www.ladder-logic.com/what-is-a-plc/

[10] Anderson, R. (2001). Why information security is hard-an economic perspective. In *Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual* (pp. 358–365). Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=991552

cheaper and easier to use remote, semi-autonomous systems than to have a human operator.[11] This results in a situation where it is in the company's interest not to update or patch hardware until it is absolutely necessary, as reaching the device is a costly process.[12] Combined with the problems discussed in the manufacturing section, this means that when a vulnerability is found it is in the best interest of the utility company to procrastinate in applying the patch as long as doing so does not affect normal operations. Similarly, the utility is incentivized to utilize existing communications infrastructure, such as publicly available telephone or Internet lines, as laying and maintaining such lines is an expensive proposition. Indeed, Figure 1 shows that over 7,000 SCADA systems are on the public Internet in the US alone.

D. Vulnerability Researchers are Incentivized to Make Attacking Easier

Attacks on IT and SCADA systems can be executed with relatively little expertise, since the vulnerability research community has made the tactics needed to execute reconnaissance and exploitation easily available. First, discovery of SCADA systems attached to the Internet has become trivial; due to recent advances in scanning technology, any individual can easily perform port scans over the entire IPv4 address space.[13] Similarly, the discovery of vulnerable systems can be done via Shodan, a database of Internet-connected devices that have been found by regular scanning. According a study cited by the Industrial Control Systems Computer Emergency Response Team (ICS-CERT), researchers have discovered over 7,200 Internet-facing SCADA systems in the US using Shodan.[14] The graphic in Figure 1 is taken from that study, each label indicating the location of an exposed control system on the Internet. Once interesting targets are found, exploitation of unpatched systems is made easier by attack tools like Metasploit. Metasploit is a system that allows a lay person with no understanding of vulnerability discovery to use prefabricated attacks to gain and maintain access to vulnerable systems.[15]

---

[11] Daneels, A., & Salter, W. (1999). What is SCADA. In *International Conference on Accelerator and Large Experimental Physics Control Systems* (pp. 339–343). Retrieved from https://accelconf.web.cern.ch/accelconf/ica99/papers/mc1i01.pdf

[12] Graham, R., & Maynor, D. (2006, January). *SCADA Security and Terrorism: We're Not Crying Wolf!* Presented at the Blackhat Security Conference, Washington, DC, USA. Retrieved from http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf

[13] Durumeric, Z., Halderman, J. A., & Eric Wustrow. (2013). ZMap: Fast Internet-Wide Scanning and its Security Applications. *Proceedings of the 22nd USENIX Security Symposium*.

[14] Industrial Control Systems Cyber Emergency Response Team. (2012). MALWARE INFECTIONS IN THE CONTROL ENVIRONMENT. *ICS-CERT Monitor*, (October/November/December 2012), 1–15

[15] Coreman, J. (2011, November 1). Intro to HDMoore's Law. *Cognitive Dissidents*. Retrieved October 22, 2013, from http://blog.cognitivedissidents.com/2011/11/01/intro-to-hdmoores-law/

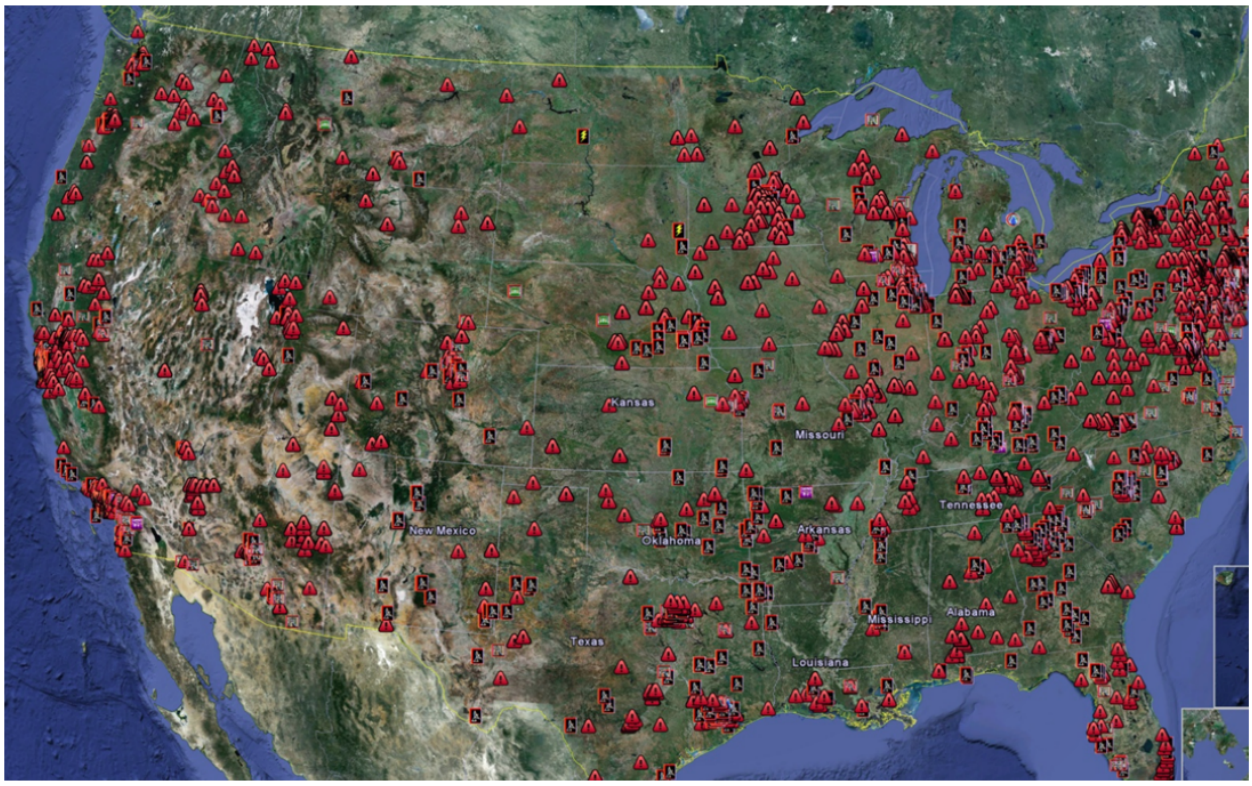

Figure 1: 7,200 Internet-facing control systems in the US found with Shodan

Vulnerability researchers are incentivized to release an exploit in a way that will enter the market without having been patched, making SCADA systems much less secure. Exploits find their way into Metasploit via a process of deskilling. Independent researchers add prepackaged exploits to Metasploit for free in a process called "full disclosure." The logic of full disclosure is that publicly advertising a vulnerability is a valuable method of forcing developers to fix bugs through public shaming without putting the discoverer at risk of lawsuit.[16] The ideal alternative, called "responsible disclosure," is when researchers disclose details about the vulnerability to manufacturers, and do not publicly release the information until after a mitigation has been provided. The issue is that this method lacks the incentive of public shaming, and leaves the researcher open for litigation. The reality is that vulnerability researchers will most often take one of two paths in releasing bugs, by either selling them or by releasing them to the public.[17] Either way, vulnerability researchers are incentivized to empower would-be attackers, making these systems less secure without remediation.

[16] Bruce Schneier. (2007, January). Schneier: Full Disclosure of Security Vulnerabilities a "Damned Good Idea." Retrieved November 8, 2013, from https://www.schneier.com/essay-146.html

[17] Frei, S., Schatzmann, D., Plattner, B., & Trammell, B. (2010). Modeling the security ecosystem-the dynamics of (in) security. In *Economics of Information Security and Privacy* (pp. 79–106). Springer. Retrieved from http://link.springer.com/chapter/10.1007/978-1-4419-6967-5_6

E. There is Need for Regulation for SCADA Systems

Security problems are endemic to computer systems in general, but SCADA systems are different in a few key ways. First, the consequences of a compromise are catastrophic compared to the risks of normal IT systems. Second, no actor in the market, from vulnerability researchers to utilities, is incentivized to responsibly disclose and fix security problems as they are discovered. Finally, security patch and update delays are exacerbated in SCADA systems compared to normal IT networks, since the systems deployed in critical infrastructure are physically remote. These factors combine to merit regulation.

Manufacturers of systems are more rationally focused on being first to market, and will allow their systems to remain insecure in pursuit of this strategy. Users of SCADA systems will fail to secure their systems due to the natural tendency to reduce costs in favor of higher efficiency. Vulnerability researchers are given reason to demonstrate that SCADA systems are insecure, and do so in such a way that provides tools to unskilled attackers. Given that these factors are likely to yield an insecure system, and the dire consequences of a successful attack, it is imperative that some regulation be drafted to raise the bar against those who would do harm to critical infrastructure.

II. PREVIOUS POLICY EFFORTS

We are not the first to view protection of critical infrastructure as a problem in need of regulation. Risks to networked critical infrastructure have been well-documented for decades, and industry and government coalitions have sought solutions for nearly as long. In this section, we survey and critique current and recent policy with regard to critical infrastructure.

Recall from the introduction that our proposed regulations consist of four key provisions:

1. Selection of an organizing agency with the power to enforce its policies and recommendations and creation of a national "red team" devoted to the continuous monitoring and assessment of critical infrastructure systems
2. A minimal common core of IT security requirements across all industries, with allowances for industry-specific policies to fit our multi-stakeholder model
3. A strong enforcement mechanism derived from financial penalties to ensure compliance with policies
4. Financial incentives for security researchers to find and responsibly disclose vulnerabilities

We find that no prior policy efforts meet all of our criteria for success, each for different reasons that we explore in this section. In Figure 2, we outline these criteria and the corresponding shortcomings of prior policy efforts. The rows comprise the regulatory measures recently pursued. The first four columns are our recommendations, and the next three are other facets of legislation that are necessary for regulation to be effective. By comprehensively studying the benefits and criticism of recent policy efforts, we gain insight into the common issues that we will avoid in our recommendations presented in Section III.

	Continuous monitoring framework (red team)	Common Core policies, as well as deference to specific industry requirements	Strong enforcement mechanism	Incentivizes responsible disclosure	Adequate civil liberties protections	Specifically addresses IT security of critical infrastructure	Implemented
CIPA / Patriot Act	✗	✗	✗	✗	✗[18]	✗	✓
CISPA	✗	✓	✗[19]	✓[20]	✗	✗	✗
SECURE IT Act	✗	✓	✗[21]	✗	✗[22]	✓	✗
Cybersecurity Act of 2012	✗	✓	✓	✓	✓	✓	✗
Exec. Order 13636 / Cybersecurity Framework	✓	✓	✗	✗	✓	✓	✓
NERC-CIP	✓	✗	✓	✗	✓	✓	✓[23]

Figure 2: Features of Competing Policy Efforts. The rows comprise the regulatory measures recently pursued. The first four columns are our recommendations, and the next three are other facets of legislation that are necessary for regulation to be effective.

[18] CIPA, the relevant portion of the Patriot Act, had no provisions for civil liberties, but also did not promote any policies that posed a significant risk to civil liberties violations. The remainder of the Patriot Act so egregious violated those liberties, however, that we grant an "x" judgment for CIPA / Patriot Act.

[19] CISPA contained no strong enforcement mechanism related to IT security of critical infrastructure because it did not present policies regulating critical infrastructure.

[20] CISPA's goals include increasing information sharing between agencies and the relevant utilities. We assume that under this scheme people would not be penalized for sharing their discoveries, but it is not out of the question.

[21] Critics primarily focus on the bill's lack of meaningful public accountability or public oversight over government agencies.

[22] Though SECURE IT's sponsors in the Senate believed that their bill contained strong civil liberties protections, groups like the EFF and CDT publicly opposed the measures because they believed that the bill presented dangerously permissive powers for the government that had a high likelihood of violating civil liberties. As such, this is a point of contention, but we believe in this matter that we should err on the side of caution, and have granted an "x".

[23] NERC-CIP is still in the process of being rolled out in its full form.

A. Recent legislation

We review the four principal legislative efforts towards securing systems in critical infrastructure from Congress during the last fifteen years: (1) The Patriot Act, (2) The Cyber Intelligence Sharing and Protection Act, (3) the SECURE IT Act, and (4) The Cybersecurity Act of 2012. Only the first (the Patriot Act) actually made it into law—the remaining proposals never made it through both houses of Congress. Some of these proposals included aspects of our key recommendations, including a coordinated effort to standardize IT security practices across industrial sectors, nominating an agency to enforce policies, and strong government-industry stakeholder partnerships. Unfortunately, each act was encumbered by other provisions, like a disappointing lack of civil liberties protections, no enforcement mechanism, or hostile government/industry relationships. The difficult history of these proposals hints at the competing interests of different stakeholders, and informs our recommendations that we present in Section IV.

1. CIPA and the Patriot Act Meet None of Our Recommendations

The relevant section of the Patriot Act, section 1016, neglects substantive regulation of computer security in computer controlled critical infrastructure, and fails to meet any of our core requirements. Section 1016, known as the Critical Infrastructure Protection Act of 2001 (CIPA), is one of the most visible responses to the attacks of September 11, 2001.

The most important consequence of CIPA was the creation of the National Infrastructure Simulation and Analysis Center (NISAC), which is tasked with "[serving] as a source of national competence to address critical infrastructure protection and continuity through support for activities related to counterterrorism, threat assessment, and risk mitigation."[24] Although NISAC is able to request and obtain data from local infrastructure assets, it can only make policy recommendations, and is unable to actually enforce any rules.

NISAC has done the technical work to prove that SCADA security is indeed a problem, publishing numerous reports[25][26] on the subject, but offers no coherent policy plan, and, by design, lacks regulatory power to force utilities to implement the technical solutions they have devised. Another key observation is the inability of NISAC-like research centers to provide incentives for utilities to improve their computer security posture. Although the establishment of a research center is unlikely to face strong political opposition, they are ineffective in implementing real policies that improve the cybersecurity of critical infrastructure. In other words, the Act inherently falls short of two of our most important policy goals: the formation of a central agency with regulatory power and implementation of

[24] H.R. 3162--107th Congress: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001. (2001). *www.GovTrack.us*. Retrieved November 24, 2013, from https://www.govtrack.us/congress/bills/107/hr3162

[25] Sandia National Laboratories: National Supervisory Control and Data Acquisition (SCADA). (n.d.). Retrieved December 9, 2013, from http://energy.sandia.gov/?page_id=859

[26] Sandia National Laboratories: SCADA Documents. (n.d.). Retrieved December 9, 2013, from http://energy.sandia.gov/?page_id=5688

strong enforcement mechanisms.

2. The Cyber Intelligence Sharing and Protection Act Demonstrates Need for Civil Liberties Protections

CISPA's approach differs from the other pieces of legislation presented here primarily in its broad information sharing provisions. This difference is also its largest drawback—it fails to address with any specificity the cybersecurity threats against critical infrastructure. Although the Act received backing from technology industry heavyweights like Microsoft, Facebook, and Apple, the information sharing provisions contained within the Act proved highly controversial with both government officials and private civil liberties advocates like the EFF, ACLU, and CDT. Given the controversial nature of these provisions, it bears understanding (1) their content and (2) the underlying motivations that compelled interested parties to react so strongly.

The bill's content focuses on enabling swift interagency communication of cybersecurity threats, but excluded targeted regulations on critical infrastructure. This approach has been criticized by many parties, and the White House addressed its shortcomings specifically in its statement of opposition on April 2, 2012:

> [CISPA] fails to provide authorities to ensure that the Nation's core critical infrastructure is protected while repealing important provisions of electronic surveillance law without instituting corresponding privacy, confidentiality, and civil liberties safeguards. For example, the bill would allow broad sharing of information with governmental entities without establishing requirements for both industry and the Government to minimize and protect personally identifiable information.[27]

Echoing the same sentiment, a coalition of academics and industry leaders signed an open letter arguing that CISPA struck a dangerous and ill-informed balance between personal privacy protections and the need for cybersecurity. Acknowledging the need for enhanced cybersecurity efforts, they admonished policymakers not to "sacrifice privacy and civil liberties" for "strong computer and network security."[28]

The White House makes a strong argument that CISPA's adoption would mark the beginning of a legislative turnaround in which the government departed from its treatment of the Internet as part of the "civilian sphere" toward an understanding of the Internet as an intelligence arena.[29]

We strongly agree with the White House that the Internet should remain in the civilian sphere. However, we also recognize that the Internet is an irresistible platform to be exploited by bad actors who desire to compromise critical infrastructure, so there is an undeniable role for intelligence to play in its protection. We emphasize that the the uninhibited sharing of private information between private corporations and governmental agencies does little to address the problems posed by critical

---

[27] EXECUTIVE OFFICE OF THE PRESIDENT: Office of Management and Budget. (2012, April 25). STATEMENT OF ADMINISTRATION POLICY H.R. 3523 - Cyber Intelligence Sharing and Protection Act.

[28] Dan Auerbach. (2012, April 23). An Open Letter From Security Experts, Academics and Engineers to the U.S. Congress: Stop Bad Cybersecurity Bills. *Electronic Frontier Foundation*. Retrieved November 7, 2013, from https://www.eff.org/deeplinks/2012/04/open-letter-academics-and-engineers-us-congress

[29] EXECUTIVE OFFICE OF THE PRESIDENT: Office of Management and Budget. (2012, April 25). STATEMENT OF ADMINISTRATION POLICY H.R. 3523 - Cyber Intelligence Sharing and Protection Act.

infrastructure cybersecurity. Therefore, we conclude that striking the appropriate balance between intelligence information sharing and privacy concerns is a further requirement in developing an implementable and successful cyber security policy.

3. SECURE IT Act Fails to Provide Regulation of Data Collection By Authoritative Agencies

The SECURE IT Act of 2012 fails to meet our requirements, on the basis of weak civil liberties protections and a lack of any clear enforcement mechanism in its policies. The act was meant to facilitate greater sharing of information between government agencies, incentivize the sharing of certain information from private businesses, more accurately define computer-related crimes on critical infrastructure, and to create a more secure network of confidential information without establishing more government oversight. It follows through with these measures, but so greatly expands upon the collection of data from commercial and private entities that it is untenable for national implementation.

Many parties had misgivings about this policy, and vehement opposition was expressed by the Electronic Frontier Foundation and others about possible civil liberties issues with the bill. Specifically, the Act lacked the necessary protections on the collection of citizens' information, and in fact removed many current restrictions on such information. The Act enables collected information to be used for a variety of purposes, whether related to imminent cybersecurity threats or not, and provides immunity to cooperative companies, giving them little incentive to protect user privacy. This relaxation on privacy restrictions is especially relevant given the history of phone wiretapping in the decade since the Patriot Act. The Act also lacked public accountability and oversight, increasing the scope of security agencies without meaningfully setting limits on their ability to pursue information.[30]

4. The Cybersecurity Act of 2012 Addresses Key Points But Failed in Congress

Perhaps the most frustrating of regulatory failures is the Cybersecurity Act of 2012; the act itself came close to supporting all of our proposed recommendations, only lacking in strong enforcement mechanisms. Praised by the EFF for being better about privacy than SECURE IT and CISPA,[31] the Act itself laid out a intelligent, top-down plan to improve the security posture of SCADA systems in critical infrastructure. Unfortunately, strong opposition from the Chamber of Commerce[32] and the climate in Congress killed the bill.[33]

The act clearly defines critical infrastructure as it pertains to SCADA systems in the same way

---

[30] Dan Auerbach. (2012, April 23). An Open Letter From Security Experts, Academics and Engineers to the U.S. Congress: Stop Bad Cybersecurity Bills. Retrieved December 9, 2013 from https://www.eff.org/deeplinks/2012/04/open-letter-academics-and-engineers-us-congress

[31] Rainey Reitman, & Lee Tien. (2012, July 19). New Cybersecurity Proposal Patches Serious Privacy Vulnerabilities. *Electronic Frontier Foundation*. Retrieved November 8, 2013, from https://www.eff.org/deeplinks/2012/07/new-cybersecurity-proposal-patches-serious-privacy-vulnerabilities

[32] Matthew Eggers. (2012, July 30). Enough With the Distractions … It's Time for Consensus-Oriented Cybersecurity Legislation. *U.S. Chamber of Commerce - Free Enterprise*. Retrieved November 7, 2013, from http://www.freeenterprise.com/enough-distractions-it-s-time-consensus-oriented-cybersecurity-legislation

[33] A farcical filibuster in which the GOP attempted to append unrelated amendments relating to abortion bans in Washington, D.C. and a repeal of Obamacare is to blame. For more on the topic, we direct the reader to (Oremus, 2012).

we defined it in Section I, and directs DHS to work with the Intelligence Community, the DOD, utilities, device manufacturers, and other stakeholders to "...conduct a top-level assessment of the cybersecurity threats, vulnerabilities, risks, and probability of a catastrophic incident across all critical infrastructure sectors to determine which sectors pose the greatest immediate risk, in order to guide the allocation of resources [for defense of critical infrastructure]…" and to do an individualized risk assessment for each specific area's use of ICS in critical infrastructure.[34] This directly matches with our recommendation for the existence of a set of core requirements, with deference to the individual necessity of each individual sector.

Although the EFF generally praised the bill, claiming that it "patched" many of the failings of prior legislation, it notes that there still may be issues. Specifically, the EFF argues that that the act, while providing much better civil liberties protections than other acts, would have allowed ISPs to unilaterally block anonymity technologies such as TOR.[35] Similarly, we find that the bill lacked enough teeth to allow DHS to force companies to comply; all recommendations made by DHS via the powers granted by this bill are voluntary. That said, the implicit threat of a future government requirement to act could actually be enough to force infrastructure companies to comply, or at least raise the bar for defense.

We and others still believe that this bill is the closest the government has come to a comprehensive solution to cybersecurity. President Obama even went as far as to write an op-ed for the Wall Street Journal in vehement support of the bill; "For the sake of our national and economic security, I urge the Senate to pass the Cybersecurity Act of 2012 and Congress to send me comprehensive legislation so I can sign it into law."[36] Unfortunately, his enthusiasm was met with disdain from the Chamber of Commerce, a major conservative lobbying group. The Chamber responded by decrying the business implications of the bill,[37] and the bill itself died by Republican filibuster, necessitating the need for an Executive Order, which resulted in Exec. Order 13636.[38]

B. Current Policy Initiatives

This section examines the most important *active* cybersecurity policy initiatives: (1) The Obama Administration's Executive Order 13636, and (2) NERC-CIP (a set of regulations for electric utilities). Neither of these initiatives implements all four of our principal recommendations, but some approach a satisfying solution. In particular, the electric utilities, via NERC-CIP, have implemented two of our

---

[34] Text of S. 2105 (112th): Cybersecurity Act of 2012 (Placed on Calendar in the Senate version). (n.d.). *GovTrack.us*. Retrieved November 7, 2013, from https://www.govtrack.us/congress/bills/112/s2105/text

[35] Rainey Reitman, & Lee Tien. (2012, July 19). New Cybersecurity Proposal Patches Serious Privacy Vulnerabilities. *Electronic Frontier Foundation*. Retrieved November 8, 2013, from https://www.eff.org/deeplinks/2012/07/new-cybersecurity-proposal-patches-serious-privacy-vulnerabilities

[36] Barack Obama. (2012, July 19). Taking the Cyberattack Threat Seriously. *The Wall Street Journal*. Retrieved from http://online.wsj.com/news/articles/SB10000872396390444330904577535492693044650

[37] Matthew Eggers. (2012, July 30). Enough With the Distractions … It's Time for Consensus-Oriented Cybersecurity Legislation. *U.S. Chamber of Commerce - Free Enterprise*. Retrieved November 7, 2013, from http://www.freeenterprise.com/enough-distractions-it-s-time-consensus-oriented-cybersecurity-legislation

[38] Engleman, E. (2012, November 14). Cybersecurity Bill Killed, Paving Way for Executive Order. *Bloomberg*. Retrieved November 25, 2013, from http://www.bloomberg.com/news/2012-11-15/cybersecurity-bill-killed-paving-way-for-executive-order.html

recommendations: a continuous monitoring framework, and a strong enforcement mechanism. We highlight these successes in order to understand the ways that we can adopt them for use beyond the electric utility sector.

In studying these two initiatives, we also observe that over 90% of critical infrastructure in the United States is owned by private corporations[39] and that the challenge to unifying a regulatory regime is enhanced by their independent nature. Consequently, achieving our principal objective of establishing a common core of regulations across sectors is perhaps the most difficult to achieve in practice.

In the remainder of this section, we distill the important aspects of each framework and use them as a guide to highlighting practical and implementable components in Section III.

1. Executive Order 13636 and the Cybersecurity Framework Lack Enforcement Mechanisms

Executive Order 13636 is a stopgap measure resulting from the failure of the Cybersecurity Act of 2012. The order directs the National Institute of Standards and Technology (NIST) and the Department of Commerce (DOC) to begin drafting a comprehensive framework that we evaluate in the remainder of this section. As a compromise, it lacks the strong enforcement mechanisms of its Congressional sibling.

The order requires the DHS to propose a plan for inter-agency and public-private information sharing, which typically raises privacy concerns regarding consumer data, and was a strong focus of all three of the failed legislative proposals. The intent of their information sharing policies is to ensure that the private operators of critical infrastructure receive relevant updates when a particular agency is aware of a vulnerability. Until the final policy framework is ready, the Order calls for the the temporary expansion of "programs that bring private sector subject-matter experts into Federal service on a temporary basis" in order to provide increased information sharing.[40]

The Obama administration seems to have gained a sensitivity for the need for privacy protections from the complaints garnered during the debate of previous bills; information sharing is constrained by the relevant privacy and civil liberties concerns, and is meticulously detailed in the report. Specifically, the DHS is ordered to include with its framework an additional privacy report to be reviewed annually by the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties.[41]

Section 7 of the Executive Order outlines the major points to be addressed in the new Framework, including compatibility with existing voluntary international and industry-specific standards, and identification of cybersecurity policies that can be applied across industry sectors. This objective is

---

[39] Keith Stouffer, Joe Falco, & Karen Scarfone. (2013, May). Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC). National Institute of Standards and Technology. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r1.pdf, Executive Summary, Page 1.

[40] Exec. Order No. 13636-- Improving Critical Infrastructure Cybersecurity. (2013, February 12). U.S. Government Printing Office. Retrieved from http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity, Section 4(e).

[41] Ibid., Section 5(b).

especially important because it approaches our central policy recommendation of creating a common core of policies—if the framework succeeds in this goal, it could form an important foundational core for future regulations. We believe that discovery of these potential cross-sector policies is critical to a successful framework because a unified set of standards encourages the development of strong common practices in equipment manufacturing, maintenance of networks, and specialization of professionals. A disjoint set of recommendations would make implementation substantially more difficult for all parties involved.

Overall, the Cybersecurity Framework initiated by Executive Order 13636, as presented in its October 22 draft form, has the potential to evolve into a useful document. Until it gains the power to enforce its own recommendations, however, it can achieve little more than facilitating a conversation among the relevant players.

2. NERC-CIP is a Strong Policy Model for a Specific Industry

In Figure 2, we claim that NERC-CIP succeeds in implementing two our of our four key policy recommendations: it instantiates a continuous monitoring framework, and it has a strong enforcement mechanism. The lacking components include the selection of a common core of cybersecurity policies across sectors, and the establishment of incentives for vulnerability researchers, both of which would be unrealistic expectations for a sector-specific body like NERC.

Importantly, NERC-CIP has been empowered to enforce its recommendations via financial means; it can fine violating utilities up to $1,000,000 for each day of violation. Their policy goals rely on quantifying and hardening "cyber assets" exposed by power companies, and they have established an implementation schedule that has already begun.[42] NERC regularly conducts live simulations of cyberattacks on utilities and monitors the defensive ability of its subjects, continually monitoring their vulnerability.[43]

As a non-profit corporation that unifies industry-wide efforts to make the North American electrical grid reliable, NERC has historically concerned itself with interfacing with the distinct power grids that cover North America. Within the last decade, however, their role has expanded to include the development and enforcement of cyber security policies across the electric power industry.

The expansion of NERC's role into a regulatory entity began when Congress passed the Energy Policy Act of 2005. This legislation mandated that FERC, the Federal Energy Regulatory Commission, certify a body to oversee the implementation of cybersecurity standards. FERC designated NERC to fill this role, and NERC-CIP is the result.

Electric utilities are an integral part of our critical infrastructure that depends on SCADA systems, and NERC-CIP has successfully created a set of correspondingly rigid cybersecurity policies with the required financial incentives. The success NERC-CIP has experienced in coordinating a public-private partnership serves as a model for other sector-specific regulation and provides the basis

[42] Kate Rowland. (2011, August). FERC versus NERC: A cyber security showdown? *Intelligent Utility*. Retrieved from http://www.intelligentutility.com/magazine/article/230725/ferc-versus-nerc

[43] Wald, M. L. (2013, November 14). Attack Ravages Power Grid. (Just a Test.). *The New York Times*. Retrieved from http://www.nytimes.com/2013/11/15/us/coast-to-coast-simulating-onslaught-against-power-grid.html

for our policy recommendation that new regulation must retain some sector-specific autonomy beyond our proposed common core.

III. OUR POLICY PROPOSALS

Our comprehensive policy proposal includes:

- The appointment of an organizing agency to set standards for computer security in critical infrastructure with a "Red Team" that has the power to investigate security vulnerabilities in live systems
- The creation of core requirements with specialization for every sector,
- The provision for financial incentives to force utilities to remediate possible threats
- The establishment of a program to actively incentivize researchers to discover and report vulnerabilities via responsible disclosure

We urge Congress to pass legislation and appropriate funds to support each of these goals. In this section we advocate for each aspect of our proposal with justifications from prior bills and analysis of actors in the market, and provide further recommendations and caveats based on emergent properties discovered in our investigations.

A. Creation of an Organizing Agency and National Red Team for Continuous Monitoring

We propose that the first step to a unified policy is the assignment or creation of an organizing agency for the implementation and maintenance of critical infrastructure SCADA security policies. Given the Department of Homeland Security's objective to secure the nation's resources and its existing incident response capabilities with ICS-CERT, we recommend that DHS fill this role. Our recommendation is not without precedent; the defeated Cybersecurity Act of 2012 appointed DHS to fill this role, and we agree that this was an appropriate choice. The authority will have to coordinate with subject matter experts in various sectors of government, academia, and industry to determine critical controls and security requirements. Individual manufacturers and utilities will need to be investigated using the agency's resources—therefore, including the subject matter experts, agencies, and firms responsible for protecting critical infrastructure is paramount.

We also suggest that a Red Team be established within the organizing agency to assess the SCADA system security of critical infrastructure providers, through continuous monitoring and penetration testing. Such a team would consist of trained attackers who play the role of malicious adversaries in order to discover existing security vulnerabilities, and an infrastructure team that would continuously monitor the external face of critical infrastructure providers. The team then can provide consistent feedback and support with regards to fixing vulnerabilities, and prescriptive changes that might alleviate some of these issues.

An alternative model that we considered (and ultimately rejected) is one in which governments require businesses to undergo processes similar to building codes, providing check-off lists and audits of the system in use. In fact, the federal government has been regulating its own networks using this kind of

auditing for years, as mandated by the Federal Information Security Management Act (FISMA). Unfortunately, this direction has been shown to be overly simplistic and therefore ineffective at actually securing networks, according to experts in the field.[44]

We instead advocate that the Red Team employ a more effective solution in which government agencies set up automated procedures that mimic attackers to reveal holes in defense. This method, known otherwise as continuous monitoring, is more realistic and can provide better security.[45] It is our belief, along with the majority of the security community, that a mandatory continuous monitoring framework paired with regular in-depth penetration testing exercises yields better security. That said, the technique requires careful and nuanced policy for an effective implementation. Such a system must be simultaneously palatable by manufacturers, critical infrastructure providers, and civil liberties groups, which typically maintain competing and unaligned interests.

1. Funding is Scalable and Worthwhile

We propose that the Red Team be structured scalably so that the number of facilities bears minimal influence on the overall costs of the organization. Similar government programs have been financially effective, and we believe that a DHS Red Team would not be any different. Continuous monitoring is easily automated and is therefore scalable; routine vulnerability scans on external infrastructure should be scalable with added resources. Additionally, the infrastructure costs required to create the scanning software and perform the scans would be minimal, especially on the scale of government operations.

In-depth penetration testing exercises are more costly and arguably less scalable, so they should be constrained by the organizing agency to reduce costs as necessary. By prioritizing targets that could prove to be the most damaging during an attack, agencies can improve their cost effectiveness with utilization of random selection; a high likelihood of inspection is enough to change the risk and cost calculus of an organization. In other words, if the critical infrastructure provider believes there is a high likelihood of government inspection, and the cost to failing such an event is high enough, the critical infrastructure provider will still be incentivized to invest in defensive measures.

Startup costs are arguably negligible, since the government has already developed the in-house expertise for such an organization. For instance, the US military and other government agencies, like the NSA, are developing or have already developed teams to continuously monitor and assess their own critical infrastructure systems to warn of immediate national security threats.[46] As mentioned in Section I,

---

[44] Jill R. Aitoro. (2011, January 28). The Fed's backward attempts at cybersecurity - Washington Business Journal. *Washington Business Journal*. Retrieved from http://www.bizjournals.com/washington/print-edition/2011/01/28/the-feds-backward-attempts-at.html

[45] Alan Paller. (2008, September 26). Paller: FISMA 2008: A better solution -- FCW. *FCW: The Business of Federal Technology*. Retrieved November 8, 2013, from http://fcw.com/articles/2008/09/26/paller-fisma-2008-a-better-solution.aspx

[46] Marcus Spade (2005). Army Approves Plan to Create School for Red Teaming. US Army Training and Doctrine Command. http://www.tradoc.army.mil/pao/tnsarchives/July05/070205.htm, accessed December 11, 2013.

DHS's ICS-CERT provides posthumous incident response support to utilities for free.[47] Similarly, details of locations and the existence of utilities are already monitored by the Environmental Protection Agency, the Department of Energy, NERC, and FERC, indicating that much of the original data collection has already been completed by the government.

2. Civil Liberties Concerns are Valid and a Barrier to Entry

Our proposal requires restriction of the targets that the Red Team may attack, the types of recommendations the Red Team may suggest, and the type of data the Red Team may collect during exercises. Furthermore, no portion of the bill may be construed to allow the restriction of general users' abilities on the Internet. For instance, this legislation may never be interpreted in such a way as to block anonymity providing services and protocols, a major consideration of the EFF.[48] These provisions will prevent government overreach, and quell fears of freedom-stifling regulation from civil liberties advocates.

The Red Team must never attempt to collect private user information, and such information, if found, must be deleted immediately. All information transferred between the regulatory agency and the company must be related to their systems and procedures, and must never include unrelated information such as personally identifiable or usage information on users or employees.

We find that prior legislative efforts, especially in the examples of SECURE IT and CISPA, demonstrated that the need for Civil liberties protections is twofold. First, protecting freedom of speech and privacy on the electronic frontier is an issue of utmost importance that deserves first class consideration. The damaging effects of a poorly thought-out remedy for security could legislate away the continued growth of the IT sector, and damage the personal liberties enjoyed today. Second, the EFF and ACLU have proven to be able to generate enough political clout to effectively bar bills from passage, indicating that civil liberties considerations are also a barrier to entry for any new consideration. Either way, it is evident that this legislation must include provisions protecting privacy and civil liberties.

B. Strong Enforcement with Financial Penalties Increases Focus on Security

Our policy proposal recommends that the organizing agency (ideally DHS, as discussed above) possess strong enforcement mechanisms to ensure that their regulations are followed. We believe that financial penalties, like the ones used by NERC-CIP, will be the most effective. This recommendation has a strong precedent to follow, as NERC-CIP derives its authority to levy fines directly from FERC, whom Congress authorized to regulate the power industry.

This proposal follows a straightforward path to increasing security in critical infrastructure by providing negative incentives for leaving them insecure. This follows directly from the market's

[47] ICS-CERT. (n.d.). Frequently Asked Questions | ICS-CERT. Retrieved December 11, 2013, from http://ics-cert.us-cert.gov/content/frequently-asked-question

[48] Rainey Reitman, & Lee Tien. (2012, July 19). New Cybersecurity Proposal Patches Serious Privacy Vulnerabilities. *Electronic Frontier Foundation*. Retrieved November 8, 2013, from https://www.eff.org/deeplinks/2012/07/new-cybersecurity-proposal-patches-serious-privacy-vulnerabilities

misaligned incentive structure as discussed in Section I; it is unlikely that critical infrastructure companies will secure their systems without incentives for change, a fact that is supported by economics research on the subject[49]. The Red Team provides this service by being given the power to fine or sue utilities in cases where they egregiously fail to provide adequate security, and in cases where critical infrastructure providers do not make enough of an effort to fix flaws found during Red Team exercises in a reasonable amount of time. Such failings are a sign of neglect on behalf of the utilities companies, and should be treated as such.

C. Incentivizing Responsible Disclosure Through Bug Bounties

We propose that the government create selective incentives for researchers to discover and disclose vulnerabilities directly to the government or to manufacturers of SCADA systems, and that manufacturers in turn be required to mitigate vulnerabilities in a reasonable time. In Section I we argue that the security of products can be drastically improved by incentivizing responsible disclosure by third parties, external to the Red Team. As discussed in the first chapter, full disclosure is the process of reporting vulnerabilities to the general public in order to publicly shame companies into fixing their products. Responsible disclosure is a similar, but improved process by which researchers will provide information on the vulnerability directly to the company responsible, and will then only publicly release information on the issue when a mitigation has been provided. This allows the manufacturer to develop and provide mitigations for vulnerabilities to the SCADA system manufacturers, which in turn may be able to apply the mitigation prior to when an adversary would be able to exercise an attack.

Specifically, our proposal is to create a national bug bounty program in which the government pays researchers for vulnerabilities in critical infrastructure in exchange for responsible disclosure. The organizing agency will then be able to provide information about the vulnerability to the manufacturer, and monitor the manufacturer's mitigation process, ensuring that the manufacturer will fix the problem.[50] Alternatively, mandating that SCADA system manufacturers provide similar bounties would be reasonable, as many other software vendors have begun to do so voluntarily. Either way, there is a legitimate market for such bugs, and researchers that discover them must be provided compensation commensurate with their work in such a way that does not result in legal action, so as to incentivize responsible disclosure.

D. Common Core of Security Requirements With Industry-Specific Policies

We recommend that the organizing agency implement a set of core requirements and metrics for success that apply to all critical infrastructure sectors, while also providing specific direction and allowances for each individual sector in critical infrastructure. A common core provides a stable security marketplace that enables standardization of technologies, increasing innovation and job portability. The security advantages discovered in one sector are easily adopted throughout all sectors of critical

[49] Oliver, P. (1980). Rewards and punishments as selective incentives for collective action: theoretical investigations. *American journal of sociology*, 1356–1375.

[50] We note that the majority of the commonly used SCADA system manufacturers exist in the US, and are under US law, see Appendix A.

infrastructure, and a disjoint set of recommendations would make implementation substantially more difficult for all parties involved.

With the above considerations in mind, we also propose that there must be a balance between providing cross-sector benefits and providing flexibility where necessary: it makes little sense to have top-down regulation without understanding each industry and how they can secure their systems in accordance with policy. Every sector has specific needs that need to be addressed individually, and experts in the Red Team can provide much needed context, and allowing the government to allot investments commensurate with importance. Our policy recommendation requires that the common core be substantial yet *minimal* in scope, striking the right balance between prescriptive regulation and multi-stakeholder industry-specific policies.

IV. CONCLUSION

This paper justifies increased regulation of the computer systems that control critical infrastructure and then proposes a comprehensive policy that address the issue directly. We accomplish the former in two ways. First, we show that the natural tendencies of all actors in the market will not provide adequate security given the dire consequences of an attack. Second, we establish that there is a lack of current functioning regulation. We propose a comprehensive set of reforms that incentivize actors in the SCADA system market to increase security, including (1) the creation of a technical team devoted to continuously monitoring SCADA systems in critical infrastructure, (2) a minimal common core of IT security requirements across all industries, with allowances for industry-specific policies to fit our multi-stakeholder model, (3) a strong enforcement mechanism derived from financial penalties to ensure compliance with policies, and (4) financial incentives for security researchers to find and responsibly disclose vulnerabilities.

In our view, legislation in this area is not only necessary, but also achievable and implementable. Providing security that may save lives should be of utmost importance, on par with strengthening defenses against other, more conventional, forms of attack. Congress routinely passes appropriation bills for conventional defense, and we urge Congress to proactively adopt our proposals for comprehensive reform of critical infrastructure SCADA security, before catastrophe necessitates it.

V. APPENDIX

A. List of Commonly Used SCADA System Manufacturers [51]

Company Name	Country of Origin
ABB	Switzerland
Advanced Control Systems (ACS)	USA
Alstom	French
C3-Ilex	USA
Citect / Schneider Electric	France
Foxboro Invensys	UK
GE Fanuc Automation	USA
GE Network Solutions	USA
Honeywell	USA
Metsoautomation (formerly Neles)	Finland
Motorola	USA
Open Systems International (OSI)	USA
QEI, Inc	USA
Siemens	Germany

B. Other Miscellaneous Regulations

Below is a list of of regulations found during the process of our analysis that we deemed unnecessary to provide a full explanation of. Our purpose here is to both demonstrate completeness and show that many have tried and failed to tackle this problem in the past.

[51] Barnes, K., Johnson, B., & Nickelson, R. (2004). Review of Supervisory Control and Data Acquisition (SCADA) Systems. *Idaho National Engineering and Environmental Laboratory*. Retrieved from http://www.inl.gov/technicalpublications/Documents/3310858.pdf

- Instrumentation, Systems, and Automation Society (ISA) / International Electrotechnical Commission (IEC); Focus is on manufacturing and control system security.
- Institute of Electrical and Electronic Engineers (IEEE); Target areas: Data and Communications, Electric Power Control and, etc.
- Government Accountability Office (GAO); Annual report: "Critical Infrastructure Protection, Challenges in Securing Control Systems"
- National Institute of Standards and Technology (NIST): Standard and guide: "System Protection Profile for Industrial Control Systems (SPP ICS)" and "Federal Information Processing Standards"
- National Infrastructure Security Coordination Centre (NISCC): Guide for SCADA and Process Control Network security[52]

[52] Cai, N., Wang, J., & Yu, X. (2008). SCADA system security: Complexity, history and new developments. In *6th IEEE International Conference on Industrial Informatics, 2008. INDIN 2008* (pp. 569–574). doi:10.1109/INDIN.2008.4618165

VI. BIBLIOGRAPHY

Abshier, J., & Marasco, P. (n.d.). Industrial Safety Standards | How Can the NERC CIP Standards Be Improved? | Control Global. Retrieved November 7, 2013, from http://www.controlglobal.com/articles/2010/nerccipstandards1012/?show=all

Alan Paller. (2008, September 26). Paller: FISMA 2008: A better solution -- FCW. *FCW: The Business of Federal Technology*. Retrieved November 8, 2013, from http://fcw.com/articles/2008/09/26/paller-fisma-2008-a-better-solution.aspx

Allen Bradley. (n.d.). What is a PLC? *Ladder Logic*. Retrieved from http://www.ladder-logic.com/what-is-a-plc/

Anderson, R. (2001). Why information security is hard-an economic perspective. In *Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual* (pp. 358–365). Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=991552

Andrew Couts. (2012, August 2). Senate kills Cybersecurity Act of 2012. *Digital Trends*. Retrieved November 7, 2013, from http://www.digitaltrends.com/web/senate-votes-against-cybersecurity-act-of-2012/

Andy Ozment. (2013, August 14). *The White House's Priorities for Cybersecurity*. Presented at the USENIX Security '13, Washington, DC, USA. Retrieved from https://www.usenix.org/conference/usenixsecurity13/white-houses-priorities-cybersecurity

Arce, I., & McGraw, G. (2004). Guest Editors' introduction: Why attacking systems is a good idea. *Security & Privacy, IEEE*, *2*(4), 17–19.

Barack Obama. (2012, July 19). Taking the Cyberattack Threat Seriously. *The Wall Street Journal*. Retrieved from http://online.wsj.com/news/articles/SB10000872396390444330904577535492693044650

Barnes, K., Johnson, B., & Nickelson, R. (2004). Review of Supervisory Control and Data Acquisition (SCADA) Systems. *Idaho National Engineering and Environmental Laboratory*. Retrieved from http://www.inl.gov/technicalpublications/Documents/3310858.pdf

Baumol, W. J. (1977). On the Proper Cost Tests for Natural Monopoly in a Multiproduct Industry. *The American Economic Review*, *67*(5), 809–822.

Bruce Schneier. (2007, January). Schneier: Full Disclosure of Security Vulnerabilities a "Damned Good Idea." Retrieved November 8, 2013, from https://www.schneier.com/essay-146.html

Byres, E. (2013). The air gap: SCADA's enduring security myth. *Communications of the ACM*, *56*(8), 29. doi:10.1145/2492007.2492018

Byres, E., & Lowe, J. (2004). The myths and facts behind cyber security risks for industrial control systems. In *Proceedings of the VDE Kongress* (Vol. 116). Retrieved from http://nealsystems.com/downloads/Myths%20and%20Facts%20for%20Control%20System%20Cyber-security.pdf

Cai, N., Wang, J., & Yu, X. (2008). SCADA system security: Complexity, history and new developments. In *6th IEEE International Conference on Industrial Informatics, 2008. INDIN 2008* (pp. 569–574). doi:10.1109/INDIN.2008.4618165

Center for Democracy and Technology. (2012). *Information Sharing, Monitoring, and Countermeasures in the Cybersecurity Act, S. 2105, and the SECURE IT Act, S. 2151* (p. 13). Retrieved from https://www.cdt.org/files/pdfs/analysis_senate_cyberbills_2012.pdf

Chertoff, M. (2009). National infrastructure protection plan. Department of Homeland Security (DHS).

Clark, D. D., & Landau, S. (2011). Untangling attribution. *Harv. Nat'l Sec. J.*, *2*, 323.

Coreman, J. (2011, November 1). Intro to HDMoore's Law. *Cognitive Dissidents*. Retrieved October 22, 2013, from http://blog.cognitivedissidents.com/2011/11/01/intro-to-hdmoores-law/

Dan Auerbach. (2012, April 23). An Open Letter From Security Experts, Academics and Engineers to the U.S. Congress: Stop Bad Cybersecurity Bills. *Electronic Frontier Foundation*. Retrieved November 7, 2013, from https://www.eff.org/deeplinks/2012/04/open-letter-academics-and-engineers-us-congress

Dan Geer. (2013). Resolved: The Internet is No Place for Critical Infrastructure. *Commun. ACM*, *56*(6), 48–53. doi:10.1145/2461256.2461273

Dan Goodin. (n.d.). Two US power plants infected with malware spread via USB drive. *Ars Technica*. Retrieved November 24, 2013, from http://arstechnica.com/security/2013/01/two-us-power-plants-infected-with-malware-spread-via-usb-drive/

Daneels, A., & Salter, W. (1999). What is SCADA. In *International Conference on Accelerator and Large Experimental Physics Control Systems* (pp. 339–343). Retrieved from https://accelconf.web.cern.ch/accelconf/ica99/papers/mc1i01.pdf

Davey, V. J., Glass, R. J., Min, H. J., Beyeler, W. E., & Glass, L. M. (2008). Effective, Robust Design of Community Mitigation for Pandemic Influenza: A Systematic Examination of Proposed US Guidance. *PLoS ONE*, *3*(7), e2606. doi:10.1371/journal.pone.0002606

David Gilbert. (2013, November 11). International Space Station Infected With USB Stick Malware Carried on Board by Russian Astronauts. *International Business Times*. Retrieved November 11, 2013, from

http://www.ibtimes.co.uk/articles/521246/20131111/international-space-station-infected-malware-russian-astronaut.htm

Derene, G. (n.d.). Inside NSA Red Team Secret Ops With Government's Top Hackers. *Popular Mechanics*. Retrieved December 11, 2013, from http://www.popularmechanics.com/technology/how-to/computer-security/4270420

Durumeric, Z., Halderman, J. A., & Eric Wustrow. (2013). ZMap: Fast Internet-Wide Scanning and its Security Applications. *Proceedings of the 22nd USENIX Security Symposium*.

Engleman, E. (2012, November 14). Cybersecurity Bill Killed, Paving Way for Executive Order. *Bloomberg*. Retrieved November 25, 2013, from http://www.bloomberg.com/news/2012-11-15/cybersecurity-bill-killed-paving-way-for-executive-order.html

Eugene Kaspersky Press Club 2013. (2013). Retrieved from http://www.youtube.com/watch?v=6tlUvb26DzI&feature=youtube_gdata_player

Exec. Order No. 13636-- Improving Critical Infrastructure Cybersecurity. (2013, February 12). U.S. Government Printing Office. Retrieved from http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

EXECUTIVE OFFICE OF THE PRESIDENT: Office of Management and Budget. (2012, April 25). STATEMENT OF ADMINISTRATION POLICY H.R. 3523 - Cyber Intelligence Sharing and Protection Act.

Frei, S., Schatzmann, D., Plattner, B., & Trammell, B. (2010). Modeling the security ecosystem-the dynamics of (in) security. In *Economics of Information Security and Privacy* (pp. 79–106). Springer. Retrieved from http://link.springer.com/chapter/10.1007/978-1-4419-6967-5_6

Graham, R., & Maynor, D. (2006, January). *SCADA Security and Terrorism: We're Not Crying Wolf!* Presented at the Blackhat Security Conference, Washington, DC, USA. Retrieved from http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf

Greg Nojeim. (2012, March 28). Cybersecurity's 7-Step Plan for Internet Freedom. *Center for Democracy and Technology*. Retrieved November 8, 2013, from https://www.cdt.org/blogs/greg-nojeim/2803cybersecuritys-8-step-plan-internet-freedom

Gus W. Weiss. (2007, April 14). The Farewell Dossier: Duping the Soviets. The Central Intelligence Agency (CIA). Retrieved from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/farewell.htm

H.R. 3162--107th Congress: Uniting and Strengthening America by Providing Appropriate Tools

Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001. (2001). *www.GovTrack.us*. Retrieved November 24, 2013, from https://www.govtrack.us/congress/bills/107/hr3162

Homeland Security Presidential Directive 7. (2003, December 17). *The Department of Homeland Security*. Retrieved November 24, 2013, from https://www.dhs.gov/homeland-security-presidential-directive-7

ICS-CERT. (n.d.). Frequently Asked Questions | ICS-CERT. Retrieved December 11, 2013, from http://ics-cert.us-cert.gov/content/frequently-asked-questions

Industrial Control Systems Cyber Emergency Response Team. (2012). MALWARE INFECTIONS IN THE CONTROL ENVIRONMENT. *ICS-CERT Monitor*, (October/November/December 2012), 1–15.

Jill R. Aitoro. (2011, January 28). The Fed's backward attempts at cybersecurity - Washington Business Journal. *Washington Business Journal*. Retrieved from http://www.bizjournals.com/washington/print-edition/2011/01/28/the-feds-backward-attempts-at.html

Kate Rowland. (2011, August). FERC versus NERC: A cyber security showdown? *Intelligent Utility*. Retrieved from http://www.intelligentutility.com/magazine/article/230725/ferc-versus-nerc

Keith Stouffer, Joe Falco, & Karen Scarfone. (2013, May). Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC). National Institute of Standards and Technology. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r1.pdf

Kraemer, S., Carayon, P., & Duggan, R. (2004). Red team performance for improved computer security. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 48, pp. 1605–1609). Retrieved from http://pro.sagepub.com/content/48/14/1605.short

Lobbying Spending Database: The US Chamber of Commerce. (n.d.). *The Center for Responsive Politics (opensecrets.org)*. Retrieved November 7, 2013, from http://www.opensecrets.org/lobby/clientsum.php?id=D000019798&year=2012

Lolita C. Baldor. (2012, February 16). Experts urge stronger cyber regulation bill. *The Washington Times*. Retrieved from http://www.washingtontimes.com/news/2012/feb/16/experts-urge-stronger-cyber-regulation-bill/

Marcus Spade. (2005, July 13). Army approves plan to create school for Red Teaming. *US Army Training and Doctrine Command*. Retrieved December 11, 2013, from http://www.tradoc.army.mil/pao/tnsarchives/July05/070205.htm

Matthew Eggers. (2012, July 30). Enough With the Distractions … It's Time for Consensus-Oriented Cybersecurity Legislation. *U.S. Chamber of Commerce - Free Enterprise*. Retrieved November 7, 2013, from http://www.freeenterprise.com/enough-distractions-it-s-time-consensus-oriented-cybersecurity-legislation

Nakashima, E. (2012, July 25). Cybersecurity bill poised for Senate consideration. *The Washington Post*. Retrieved from http://www.washingtonpost.com/world/national-security/cybersecurity-bill-poised-for-senate-consideration/2012/07/24/gJQAZxpU7W_story.html

Nicolas Falliere, Eric Chien, & Liam O Murchu. (2011). *W32.Stuxnet Dossier* (Security Response No. 1.4). Symantec. Retrieved from http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Oremus, W. (2012, August 2). Republicans Filibuster Cybersecurity Bill With Anti-Abortion, Obamacare Amendments. *Slate*. Retrieved from http://www.slate.com/blogs/future_tense/2012/08/02/cybersecurity_act_republicans_filibuster_lieberman_bill_with_abortion_obamacare_amendments.html

Rainey Reitman. (2012, April 26). Even with Rogers' Amendments, CISPA is Still a Surveillance Bill. *Electronic Frontier Foundation*. Retrieved November 7, 2013, from https://www.eff.org/deeplinks/2012/04/even-rogers-amendments-cispa-still-surveillance-bill

Rainey Reitman, & Lee Tien. (2012, July 19). New Cybersecurity Proposal Patches Serious Privacy Vulnerabilities. *Electronic Frontier Foundation*. Retrieved November 8, 2013, from https://www.eff.org/deeplinks/2012/07/new-cybersecurity-proposal-patches-serious-privacy-vulnerabilities

Russia: Hidden chips "launch spam attacks from irons." (2013, October 28). *BBC*. Retrieved from http://www.bbc.co.uk/news/blogs-news-from-elsewhere-24707337

S. 2105--112th Congress: Cybersecurity Act of 2012. (2012). *GovTrack.us*. Retrieved November 8, 2013, from https://www.govtrack.us/congress/bills/112/s2105

Sandia National Laboratories: National Supervisory Control and Data Acquisition (SCADA). (n.d.). Retrieved December 9, 2013, from http://energy.sandia.gov/?page_id=859

Sandia National Laboratories: SCADA Documents. (n.d.). Retrieved December 9, 2013, from http://energy.sandia.gov/?page_id=5688

Sen Franken Backs Cybersecurity Alternative To CISPA & SECURE IT. (2012). Retrieved from https://www.youtube.com/watch?v=x72q7PgaZvk&feature=youtube_gdata_player

Shackelford, S. J. (2012). In Search of Cyber Peace: A Response to the Cybersecurity Act of 2012. *Stanford Law Review Online*, *64*, 106.

Spina, S. M., & Skees, J. D. (n.d.). *Electric Utilities and the Cybersecurity Executive Order: Anticipating the Next Year*.

Text of S. 2105 (112th): Cybersecurity Act of 2012 (Placed on Calendar in the Senate version). (n.d.). *GovTrack.us*. Retrieved November 7, 2013, from https://www.govtrack.us/congress/bills/112/s2105/text

The National Institute of Standards and Technology (NIST). (2013, October 22). *NIST Releases Preliminary Cybersecurity Framework, Will Seek Comments: Contact: Jennifer Huergo*. Press Release. Retrieved from http://www.nist.gov/itl/cybersecurity-102213.cfm

US Department of Commerce, N. (n.d.). Press Briefing, Preliminary Cybersecurity Framework. Retrieved November 6, 2013, from http://www.nist.gov/director/speeches/cybersecurity-framework-remarks-102213.cfm

Wald, M. L. (2013, November 14). Attack Ravages Power Grid. (Just a Test.). *The New York Times*. Retrieved from http://www.nytimes.com/2013/11/15/us/coast-to-coast-simulating-onslaught-against-power-grid.html

William Safire. (2004, February 2). The Farewell Dossier. *New York Times*. Retrieved from http://www.nytimes.com/2004/02/02/opinion/the-farewell-dossier.html

Zhu, B., Joseph, A., & Sastry, S. (2011). A Taxonomy of Cyber Attacks on SCADA Systems. In *Proceedings of the 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing* (pp. 380–388). Washington, DC, USA: IEEE Computer Society. doi:10.1109/iThings/CPSCom.2011.34