ACKNOWLEDGING THE THREAT: SECURING UNITED STATES PIPELINE SCADA SYSTEMS

Synopsis: The threat of large-scale cyber attacks on the nation's oil and gas pipeline SCADA systems is increasing. Despite the growing threat, pipeline SCADA systems remain wanting in the area of cybersecurity. However, the newly created NIST Framework and the ONG-C2M2 model combine to lay a strong foundation for the development of increased cybersecurity in the oil and gas pipeline sectors. With increased information sharing between the private sector and the government, and specific, numeric objectives to work toward in developing cybersecurity programs for pipeline SCADA systems, the voluntary measures currently in place might prove effective in protecting systems nationwide. These voluntary measures could be strengthened through legislation streamlining the information sharing process and providing liability and privacy protection for oil and gas pipeline owners, which would further incentivize industry participation.

I. INTRODUCTION

Although the United States has recently focused heavily on foreign policy and international economic stability, cybersecurity in the oil and gas industries may have been neglected due to generational differences in recognizing the threats that cyber vulnerabilities can create.[1] The 2003 electrical blackout and the 2010 discovery of the malware known as Stuxnet caused the electric grid and nuclear systems to receive attention in recent years, but cybersecurity of oil and natural gas pipelines has not received the same attention.[2] Some sources report that oil and gas companies lose as much as $8.4 million per day due to cyber attacks.[3]

Many pipelines today are controlled by computerized Supervisory Control and Data Acquisition (SCADA) systems. SCADA systems have been criticized as non-standardized and vulnerable to cyber attacks.[4] Currently, the U.S. Department of Homeland Security (DHS)—in conjunction with the U.S. Department of Transportation's (DOT) Pipeline and Hazardous Materials Safety Administration (PHMSA)—monitors pipeline security through the Transportation Security Administration (TSA).[5] Some argue that DHS lacks adequate resources and has struggled with regulations to promulgate SCADA standards, leading to a discretionary mix of security efforts.[6] This comment suggests that the newly introduced National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (Framework), combined with the Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-

[1] Dominic Basulto, *When Will Cybersecurity Become a Major Campaign Issue?*, WASH. POST (Nov. 5, 2013), http://www.washingtonpost.com/blogs/innovations/wp/2013/11/05/when-will-cybersecurity-become-a-major-campaign-issue/.

[2] Bruce Schneier, *The Story Behind the Stuxnet Virus*, FORBES (Oct. 7, 2010), http://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html (noting that Stuxnet exerted control over Iranian nuclear centrifuges without immediate detection); Bryan Walsh, *10 Years After the 2003 Blackout, Is the Grid Ready for Disaster?*, TIME (Aug. 13, 2013), http://science.time.com/2013/08/13/ten-years-after-the-great-blackout-the-grid-is-stronger-but-vulnerable-to-extreme-weather/.

[3] STEWART BAKER, NATALIA FILIPIAK & KATRINA TIMLIN, IN THE DARK: CRUCIAL INDUSTRIES CONFRONT CYBERATTACKS 9, 10 (McAfee 2011) [hereinafter IN THE DARK], *available at* http://www.mcafee.com/uk/resources/reports/rp-critical-infrastructure-protection.pdf.

[4] NAT'L TRANSP. SAFETY BD., NTSB/SS-05/02, SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) IN LIQUID PIPELINES 1, 2, 3 (2005) [hereinafter SCADA IN LIQUID PIPELINES], *available at* http://www.ntsb.gov/doclib/safetystudies/SS0502.pdf.

[5] Elisabeth R. Myers, *Oil Pipelines*, 2010 A.B.A. RECENT DEV. PUB. UTIL. COMM. & TRANSP. i, 16 (2010), *available at* http://0-www.heinonline.org.library.utulsa.edu/HOL/Page?handle=hein.journals/pubutili2010&div=8&collection=journals&set_as_cursor=0&men_tab=srchresults&terms=elisabeth|myers|oil|pipelines&type=matchall#2.

[6] PAUL W. PARFOMAK, CONG. RESEARCH SERV., R42660, PIPELINE CYBERSECURITY: FEDERAL POLICY (2012) [hereinafter PIPELINE CYBERSECURITY], *available at* http://www.fas.org/sgp/crs/homesec/R42660.pdf; DEP'T OF HOMELAND SEC., OFFICE OF THE INSPECTOR GEN., OIG-14-02, DHS' EFFORTS TO COORDINATE THE ACTIVITIES OF FEDERAL CYBER OPERATIONS CENTERS 1 (2013) [hereinafter DHS' EFFORTS TO COORDINATE], *available at* http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-02_Oct13.pdf; Tony Romm, *IG: DHS Cybersecurity Tools, Training Not Up to Par*, POLITICO (Nov. 5, 2013), http://www.politico.com/story/2013/11/homeland-security-cybersecurity-99347.html; Daniela Oliveira, *Cyber-Terrorism & Critical Energy Infrastructure Vulnerability to Cyber-Attacks*, 5 ENVTL. & ENERGY L. & POL'Y J. 519, 521 (2010) [hereinafter *Cyber-Terrorism*] (citing STEWART BAKER, CTR. FOR STRATEGIC & INT'L STUDIES, IN THE CROSSFIRE: CRITICAL INFRASTRUCTURE IN THE AGE OF CYBER WAR 22 (2010) [hereinafter IN THE CROSSFIRE], *available at* http://img.en25.com/Web/McAfee/NA_CIP_RPT_REG_2840.pdf); IN THE DARK, *supra* note 3, at 19; Darlene Storm, *10 Years Later, DHS Still Plagued with Cybersecurity, Critical Infrastructure Problems*, COMPUTER WORLD (Sept. 11, 2013) [hereinafter *10 Years Later*], http://blogs.computerworld.com/cybercrime-and-hacking/22800/10-yrs-later-dhs-still-plagued-cybersecurity-critical-infrastructure-problems.

C2M2) put forth by DHS and the U.S. Department of Energy (DOE), creates a solid foundation for pipeline SCADA system cybersecurity that DHS can utilize as it intensifies its standardization efforts in the oil and gas industry.[7]

II. BACKGROUND

A. *SCADA Systems in Oil and Gas Pipelines*

Liquid and gas transmission pipelines span far enough to circle the globe seven and twelve times, respectively, and they transport nearly two-thirds of the United States' energy supply.[8] Gas distribution pipelines span an additional 1.9 million miles throughout the United States, creating a vast national pipeline network.[9] Technological advances over the past decade have reduced the cost of SCADA systems, allowing virtually uniform use of SCADA technology throughout interstate pipelines.[10] Through SCADA, the industry can control thousands of miles of pipeline from one central location.[11] Human controllers can input commands to remotely operate pipeline control equipment.[12] These instruments relay critical measurements such as pressure, temperature, and rate of oil or gas flow back to the main control computer via remote terminal units, and indicate any change in status along the pipelines so that human controllers can maintain pipeline stability.[13]

Although there are numerous SCADA software packages, most SCADA systems contain a three-layer architecture that may be analyzed as a *data layer*, a *processing layer*, and a *user interface layer*.[14] The *processing layer* gathers data from remote terminal units, storing it in the *data layer*, and issues commands to controls along the pipeline to change or maintain their states.[15] The *user interface layer's* capabilities depend on human response to data, with the human controller receiving data through the *processing* and *data layers* on monitors in the central

[7] *See generally* NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (2014) [hereinafter NIST FRAMEWORK], *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf; DEP'T OF ENERGY & DEP'T OF HOMELAND SEC., OIL & NATURAL GAS SUBSECTOR CYBERSECURITY CAPABILITY MATURITY MODEL (ONG-C2M2) (2014) [hereinafter CYBERSECURITY MODEL], *available at* http://energy.gov/sites/prod/files/2014/03/f13/ONG-C2M2-v1-1_cor.pdf.

[8] Myers, *supra* note 5, at 15. Liquid pipelines span roughly 170,000 miles across the country while gas transmission pipelines measure 295,000 miles. Paul Butterworth & David Palmer, *Ask an Astrophysicist*, NAT'L AERONAUTICS & SPACE ADMIN. (Apr. 1, 1997), http://imagine.gsfc.nasa.gov/docs/ask_astro/answers/970401c.htm.

[9] Myers, *supra* note 5, at 15.

[10] SCADA IN LIQUID PIPELINES, *supra* note 4, at 1.

[11] *Id.*

[12] *Id.* This equipment includes flow meters, pressure transmitters, temperature transmitters, valves, pumps, and other control units. *Id.*

[13] *Id.*

[14] Nary Subramanian, *Improving Security of Oil Pipeline SCADA Systems Using Service-Oriented Architectures*, ON THE MOVE TO MEANINGFUL INTERNET SYSTEMS (OTM), 344, 345 (2008), *available at* http://www.uttyler.edu/cs/documents/subramanian.pdf.

[15] *Id.*

control station and instructing the processing layer to control valves and pumps as needed.[16]

Extensive pipeline systems mandate extensive networks, making them vulnerable.[17] Originally, SCADA systems did not have such expansive networks, and developed in open network environments with minimal security features.[18] Because of existing vulnerabilities, however, one source reported that currently the rate of victimization is highest in the oil and gas industry with 31% of industry members having purportedly been attacked, and the power sector close behind at 27%.[19] Of the 245 cyber incidents reported to DHS's National Cybersecurity and Communications Integration Center (NCCIC) in a five month period, 79 were in the energy sector.[20]

Distributed Denial of Service (DDoS) attacks are popular. Two-thirds of oil and gas executives reported such intrusions with one-third of industry leaders polled reporting DDoS attacks within their SCADA systems.[21] Over 50% of cyber attacks launched on the oil and gas industry are aimed at SCADA systems, costing companies an estimated $8.4 million per day.[22]

B. Pipeline SCADA System Vulnerabilities

1. Vulnerable Equipment

Communication connections over external networks and the Internet encourages the use of devices that were not designed for remote operation and that

[16] *Id.*

[17] BLAKE CLAYTON & ADAM SEGAL, COUNCIL ON FOREIGN RELATIONS, ADDRESSING CYBER THREATS TO OIL AND GAS SUPPLIERS 2-3 (2013) [hereinafter ADDRESSING CYBER THREATS], *available at* http://www.cfr.org/cybersecurity/addressing-cyber-threats-oil-gas-suppliers/p30977. For example, in an attack by Chinese hackers known as "Night Dragon," infiltrators stole gigabytes of highly sensitive proprietary material from oil and gas corporations. *Id.* Other potential exploitations of vulnerabilities include attacks on offshore oil rigs causing environmental disasters, explosions triggered by malware in SCADA systems on oil or natural gas pipelines, or the paralysis of tens of thousands of system computers so as to render oil and gas corporations inoperable. *Id.*

[18] IN THE CROSSFIRE, *supra* note 6, at 22. These open network environments included the Internet or Internet Protocol (IP) networks. *Id.*

[19] *Id.* at 8. "Victimization" is defined as "making a victim of someone, or harming or committing a crime against someone." *Victimize Definition*, MERRIAM-WEBSTER.COM, http://www.merriam-webster.com/dictionary/victimize (last visited Apr. 14, 2015).

[20] *Incident Response Activity*, ICS-CERT MONITOR (2015), *available at* https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf.

[21] IN THE CROSSFIRE, *supra* note 6, at 5, 6-7, 9. The transportation sector, in comparison, only had half of its executives report DDoS attacks. *Id.* at 7. DDoS attacks occur when attackers flood a target source—usually a website—with large amounts of traffic, often generated through a network of infected computers known as a "botnet." Gary Davis, *Visualizing a DDoS Cyber Attack*, MCAFEE BLOGS (Apr. 29, 2013), http://blogs.mcafee.com/consumer/consumer-threat-notices/visualizing-a-ddos-cyber-attack.

[22] IN THE CROSSFIRE, *supra* note 6, at 9, 10. Costs stem from downtime associated with a major cybersecurity incident, which is considered to be one that "causes severe loss of services for at least 24 hours, loss of life or personal injury, [or] failure of a company." *Id*. at 10. There is often an expectation that these costs will be born by insurers, rate-payers, or customers, although this expectation is less widespread in the oil and gas sector. *Id.*

lack native security.[23] As the central control stations attempt to connect with peripherals, they transit networks with many unsecured access points.[24] Only 35% of industry experts report monitoring their control system protocols—or the methods by which their devices communicate with each other—leaving these natively insecure protocols vulnerable to third-party intervention.[25]

2. Vulnerabilities from Connectivity

Most vulnerabilities arise from linking SCADA networks to the Internet.[26] Due to exposure to unsecured elements of the Internet, communication channels become exposed to network attacks from many angles.[27] As of 2013, an investigation by DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) determined that more than 7,200 devices directly related to control systems of industrial equipment were accessible via the Internet, and that many of these devices had "weak, default or nonexistent logon credential requirements."[28]

Some vulnerabilities are even available in the public domain, with hackers publishing source code, intrusion techniques, and system attack points online once they have successfully infiltrated a corporate system so that others may follow suit.[29] The same Internet that permits SCADA connectivity permits SCADA networks' exploitation.

3. Vulnerable Applications

Third-party applications such as web servers, databases, and encryption services may be unsecure or lacking in current updates, which creates more attack points for hackers.[30] Additionally, connection of SCADA systems with other corporate applications may create efficiency but add vulnerability.[31]

4. Large-Scale Vulnerabilities

Access to a protected network may permit access to attached applications.[32] Even with the use of firewalls, air gaps, and other security measures, linking a

[23] MATTHEW E. LUALLEN, SANS SCADA AND PROCESS CONTROL SECURITY SURVEY 1, 9 (2013) [hereinafter SANS SCADA], *available at* https://www.sans.org/reading-room/analysts-program/sans-survey-scada-2013.

[24] *Id.*

[25] *Id.* Protocols are the method by which equipment, digital controllers, software, and external systems communicate within an industrial control network. BRENDAN GALLOWAY & GERHARD P. HANCKE, INTRODUCTION TO INDUSTRIAL CONTROL NETWORKS 1 (2012), *available at* http://foresight.ifmo.ru/ict/shared/files/201311/1_135.pdf.

[26] IDAHO NAT'L LAB., NSTB ASSESSMENTS SUMMARY REPORT: COMMON INDUSTRIAL CONTROL SYSTEM CYBERSECURITY WEAKNESSES 34 (2010) [hereinafter NSTB ASSESSMENTS], *available at* https://www.fas.org/sgp/eprint/nstb.pdf.

[27] *Id.*

[28] Rachael King, *Report: Cyber Threats to Energy Sector Happening at 'Alarming Rate*,' WALL ST. J. (Jan. 2, 2013), http://blogs.wsj.com/cio/2013/01/02/report-cyber-threats-to-energy-sector-happening-at-alarming-rate/.

[29] NSTB ASSESSMENTS, *supra* note 26, at 34.

[30] *Id.* at 35-36.

[31] *Id.* at 36-37.

[32] *Id.*

corporate database containing customer data to the SCADA network may allow an attacker who previously obtained access to the SCADA system to gain access to the corporate database, providing a window through which he can gain access throughout the enterprise.[33]

Alternatively, an attacker with access to the corporate network might be able to obtain access to an interstate pipeline SCADA system.[34] It was reported that in 2003, the Structured Query Language (SQL) Slammer worm gained access to the SCADA system at Ohio's Davis-Besse nuclear power plant through a business network, causing the crash of a computerized system of safety indicators.[35]

5. "Man in the Middle" Vulnerabilities

A "Man in the Middle" (MitM) attack occurs when an attacker gains access to two peripheral points on the network, such as a computer or pipeline pump, and intercepts communications between them without either peripheral point detecting the interception.[36] A MitM attack requires falsification of the identity of each peripheral point so that neither point realizes that the communications are being intercepted.[37] This seemingly complicated access can be quite simple if the SCADA system lacks adequate methods to insure the identity of the partner or the integrity of the message.[38]

A MitM attack enables complete control of the data flowing between system components.[39] An attacker could manipulate commands and messages being sent to field equipment and to operator screens, and allow physical control of the pipeline while altering the operator's view.[40]

6. Stolen Credentials

Capture of a legitimate user's username and password can allow an attacker to log onto the system with that user's privileges.[41] A system administrator or controller's credentials could give the hacker complete control of the valves, pumps, instruments, and other peripheral equipment throughout the pipeline.[42]

[33] *Id.* at 50. Although some cyber attacks, such as the Shamoon virus attack on Saudi Arabian Oil Co. in 2012, were mitigated thanks to security measures that kept the corporate network and the control system network separate, hackers have discovered several ways to bypass air gaps, including through the use of USB devices to transport devices. This method was utilized to spread the Stuxnet virus to Iranian nuclear centrifuges in 2013. King, *supra* note 28.

[34] NSTB ASSESSMENTS, *supra* note 26, at 50.

[35] *SCADA Systems and the Terrorist Threat: Protecting the Nation's Critical Control Systems*, 109th Cong. 20 (2005) [hereinafter *SCADA Systems and the Terrorist Threat*], *available at* http://www.fas.org/irp/congress/2005_hr/scada.pdf (statement of Samuel G. Varnado, Dir., Sandia Nat'l Labs). SQL is the standard language for querying databases. *What is SQL, and What are Some Example Statements for Retrieving Data from a Table?*, IND. UNIV. (Apr. 1, 2015), *available at* https://kb.iu.edu/d/ahux.

[36] NSTB ASSESSMENTS, *supra* note 26, at 40.

[37] *Id.*

[38] *Id.* Many SCADA systems do not offer these identity or integrity authentications, leaving the networks vulnerable to MitM attacks at every point. *Id.* at 40-41.

[39] *Id.* at 43.

[40] *Id.*

[41] NSTB ASSESSMENTS, *supra* note 26, at 41.

[42] *Id.* at 42.

This access might go unnoticed for some time if other controllers believe that an authorized user is making the system changes.[43]

A "spear-phishing attack," which preys on the lack of cybersecurity knowledge of control system personnel, tricks the true operator into entering his password.[44] Human controllers may also fail to protect their credentials through passwords that are easy to crack, providing an easy and quick way for attackers to gain access to the system.[45] Further, human controllers are often given more administrator privileges than needed.[46]

C. *Cyber Attacks on Oil and Gas Pipelines*

SCADA system failures in the energy sector are not new, and many have resulted in significant consequences.[47] A deliberate, more calculated cyber attack on a SCADA system might have the same or worsened consequences. Based on recent events, cyber attacks on SCADA systems seem to be increasing in frequency. In the summer of 2008, an attacker hacked Marathon Oil, ExxonMobil, and ConocoPhillips, stealing data regarding the quantity, value, and location of oil discoveries worldwide.[48] In 2010, Stuxnet—one of the most sophisticated and renowned cyber attacks on an industrial control system to date—was discovered in Iranian nuclear control systems, as well as in Indonesia and other peripheral countries.[49] The Stuxnet malware attacked Windows systems and was deployed using infected removable media.[50] The malware spread quickly using exploits, infecting computers inside private networks.[51] Ultimately, the malware made its

[43] *Id.* at 41.

[44] SANS SCADA, *supra* note 23, at 4; NSTB ASSESSMENTS, *supra* note 26, at 54.

[45] NSTB ASSESSMENTS, *supra* note 26, at 61. For example, when a controller uses the word "password" as his or her password.

[46] *Id.* at 63.

[47] *SCADA Systems and the Terrorist Threat*, *supra* note 35. In 1982, Trojans installed SCADA system equipment that was allegedly intercepted before its delivery to the former Soviet Union caused the Trans-Siberian Pipeline to explode. *Id.* at 16-17. In 1988, the Piper Alpha North Sea Platform exploded after a loss of control over the industrial control system, killing 167 people and resulting in $15.2 billion in losses. *Id.* at 84. Then, in June 1999, an oil pipeline in Bellingham, Washington, ruptured due to a faulty use of the SCADA system, releasing 237,000 gallons of gasoline into a creek, igniting and burning for one and a half miles, killing three youths, injuring eight individuals, and causing $45 million in damage. *Id.* at 91-92. Finally, in 2005, faulty SCADA signals and indicators caused an explosion at the Texas City oil refinery, killing fifteen, injuring 170, and causing nearly $1 billion in damage. *Id.* at 84.

[48] CTR. FOR STRATEGIC & INT'L STUDIES, SIGNIFICANT CYBER INCIDENTS SINCE 2006 3 (2014) [hereinafter SIGNIFICANT CYBER INCIDENTS], *available at* http://csis.org/files/publication/140310_Significant_Cyber_Incidents_Since_2006.pdf.

[49] *Id.* at 7.

[50] PHILIP A. CRAIG, JR. & THOMAS P. MCKENNA, JR., PAC. NW. NAT'L LAB., TECHNOLOGY SECURITY ASSESSMENT FOR CAPABILITIES AND APPLICABILITY IN ENERGY SECTOR INDUSTRIAL CONTROL SYSTEMS: MCAFEE 34-35 (2012), *available at* http://www.mcafee.com/us/resources/reports/rp-energy-sector-industrial-control.pdf (citing N. AM. ELEC. RELIABILITY COUNCIL, TOP 10 VULNERABILITIES OF CONTROL SYSTEMS AND THEIR ASSOCIATED MITIGATIONS (2006), *available at* http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/NERC_2007_Top_10.pdf.

[51] *Id.* An exploit involves a virus exploiting a security flaw of a system or application in order to invade that system and spread to new systems. ERIC CHIEN & PETER SZOR, SYMANTEC, BLENDED ATTACKS EXPLOITS, VULNERABILITIES AND BUFFER-OVERFLOW TECHNIQUES IN COMPUTER VIRUSES 3 (2002), *available at* https://www.symantec.com/avcenter/reference/blended.attacks.pdf.

way into a uranium enrichment plant, affecting the spinning speed of centrifuges and causing industrial control equipment to fail.[52]

In November 2011, at least ten large Norwegian defense and energy companies were hacked after attackers stole credentials using a spear-phishing scheme, allowing them to gain access to confidential documents, industrial data, usernames, and passwords.[53] In early 2012, information regarding industrial control systems throughout the United States was discovered on captured al-Qaeda computers.[54] DHS subsequently issued warnings in March 2012 regarding a cyber intrusion campaign on U.S. gas pipelines that had begun in December 2011.[55] The spear-phishing attack targeted twenty-three gas pipeline companies and was thought to originate with China's military hacking units.[56]

McAfee, a computer security company, discovered another attack on the oil and gas sector shortly thereafter, naming it "Night Dragon."[57] The attack had been ongoing from 2008 until 2011, and appeared to be a coordinated campaign by Chinese hackers to obtain data from five major western energy companies.[58] The hackers were able to steal a significant amount of highly confidential data, including proprietary information about oil and gas pipeline operations.[59] This information could later be used to design an attack on U.S. pipeline systems.[60]

In mid-2012, a cyber attack targeting internal computer systems forced Iran to take key oil facilities offline.[61] The malware was placed inside the control systems of Iran's main oil exporting terminal, and it was able to glean user data from the network.[62] Further, although Iran claimed that oil production was not affected, several Iranian oil plants were completely disconnected from the Internet as a precaution, causing degradation in service and financial losses.[63]

In May 2012, the Iranian oil industry was the victim of another attack when an espionage-oriented cyber tool named "Flame" was discovered in Iranian Oil Ministry computers.[64] Shortly thereafter, in August 2012, a hacking group used a virus named "Shamoon" to attack Aramco, one of the largest Saudi oil suppliers.[65]

[52] ADDRESSING CYBER THREATS, *supra* note 17, at 2-3.

[53] SIGNIFICANT CYBER INCIDENTS, *supra* note 48, at 10-11.

[54] *SCADA Systems and the Terrorist Threat*, *supra* note 35, at 32.

[55] SIGNIFICANT CYBER INCIDENTS, *supra* note 48, at 10-11.

[56] Mark Clayton, *Cyberattack Leaves Natural Gas Pipelines Vulnerable to Sabotage*, CHRISTIAN SCI. MONITOR (Feb. 27, 2013), http://www.csmonitor.com/Environment/2013/0227/Exclusive-Cyberattack-leaves-natural-gas-pipelines-vulnerable-to-sabotage; SIGNIFICANT CYBER INCIDENTS, *supra* note 48, at 10-11.

[57] ADDRESSING CYBER THREATS, *supra* note 17, at 1-2.

[58] *Id.*

[59] *Id.*

[60] Elizabeth MacDonald, *U.S. Oil and Gas at Greater Risk for Cyber Attacks*, FOX BUS. (June 26, 2013), http://www.foxbusiness.com/technology/2013/06/26/us-oil-and-gas-at-greater-risk-for-cyber-attacks/.

[61] SIGNIFICANT CYBER INCIDENTS, *supra* note 48, at 11.

[62] *Id.*

[63] *Id.*

[64] *Id.* The code set was also discovered in Israel, Syria, and Sudan, in addition to several other countries outside of the Middle East. *Id.*

[65] *Id.* at 12.

The virus deleted data on over 30,000 computers and infected the oil company's SCADA systems.[66]

In December 2014, experts determined that a pipeline explosion in Turkey in 2008 was caused by a cyber attack.[67] The attackers hacked into the pipeline's surveillance cameras, which were connected to the control system network.[68] From the cameras, they were able to shut down alarms, cut off communications between the pipeline and the control room, jam the backup satellite communications, erase all surveillance footage, and super-pressurize the crude oil in the pipeline until it exploded.[69] Because all sensors and automated emergency mechanisms had been disabled, the control room did not discover the explosion until a security worker saw the flames forty minutes after it occurred.[70] More than 30,000 barrels of oil spilled above a water aquifer, and the incident cost eleven companies—including BP and Chevron—more than $5 million per day in transit tariffs.[71] The State Oil Fund of the Republic of Azerbaijan also ultimately lost $1 billion in export revenue.[72]

As cyber attacks do not require the wealth and resources of traditional military attacks, they can be utilized by poorer nations or rogue organizations, and victims are provided little to no forewarning.[73] Consequently, anticipating the scale of a SCADA system attack and preparing an adequate response to handle its aftermath become formidable tasks.[74] Nevertheless, nation-states have been the predominant attackers in recent years.[75] For example, in May 2013, the Wall Street Journal reported that Iranian nationals specifically intensified their efforts to compromise U.S. utility providers.[76]

D. Existing Cybersecurity Standards

There has not yet been significant formal regulation on the issue of standardized cybersecurity measures for pipeline SCADA systems.[77] In 1993, the

[66] SIGNIFICANT CYBER INCIDENTS, *supra* note 48, at 12. The attack also affected other oil companies, including RasGas in Qatar—a major liquefied natural gas supplier. *Id.*

[67] Jordan Robertson & Michael Riley, *Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar*, BLOOMBERG BUS. (Dec. 10, 2014), http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar.

[68] *Id.*

[69] *Id.*; ROBERT LEE, MICHAEL ASSANTE, AND TIM CONWAY, SANS INDUSTRIAL CONTROL SYSTEMS, MEDIA REPORT OF THE BAKU-TBILISI-CEYHAN (BTC) PIPELINE CYBER ATTACK 5 (2014), *available at* https://ics.sans.org/media/Media-report-of-the-BTC-pipeline-Cyber-Attack.pdf.

[70] Robertson & Riley, *supra* note 67.

[71] *Id.*

[72] *Id.*

[73] Clay Wilson, *Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, NAVY DEP'T LIBRARY (Apr. 1, 2005), http://www.history.navy.mil/library/online/computerattack.htm.

[74] *Id.*

[75] MacDonald, *supra* note 60.

[76] *Id.* at 14.

[77] *DHS Cybersecurity: Roles and Responsibilities to Protect the Nation's Critical Infrastructure*, 113th Cong. 4 (2013) [hereinafter *DHS Cybersecurity*], *available at* http://www.gpo.gov/fdsys/pkg/CHRG-113hhrg81458/html/CHRG-113hhrg81458.htm (statement of Hon. Michael T. McCaul, Chairman, H. Comm. on Homeland Sec.). While there has been little formal legislation regarding pipeline SCADA systems, the U.S. House of Representatives did recently pass the Protecting Cyber Networks Act, which creates a system of

American Petroleum Institute (API) developed a set of general guidelines for companies to consider when developing control room standards, but did not include any standardization requirements.[78] However, there have been significant efforts toward creating a public-private partnership to reduce vulnerabilities, initiated by a presidential directive issued by President Clinton in May 1998.[79] The directive also named DOT as the lead agency for the pipeline sector and DOE as the sector liaison for oil and gas production and storage.[80]

Shortly after the northeastern blackout in 2003, Homeland Security Presidential Directive 7 was released, instructing the Secretary of Homeland Security to establish uniform policies, approaches, guidelines, and methodologies for integrating federal infrastructure protection across sectors, which included pipeline systems.[81] This provided for shared control of pipeline security standards between DOT, the newly founded DHS, and the private sector.[82]

In 2006, DHS released LOGIIC, a system developed through a public and private partnership designed to serve as a cybersecurity tool for the oil and gas industry.[83] However, a study conducted by McAfee determined that more than one-third of IT executives in the electric, oil, gas, and water industries in the United States reported no contact at all with the government regarding their cybersecurity standards.[84] As of 2010, the government was not auditing companies' security plans on a widespread basis, with audit rates hovering below 20%.[85]

Over the past few years, cybersecurity initiatives for pipeline SCADA systems have been split between TSA (under DHS), DOE, and DOT.[86] The Pipeline Inspection, Protection, Enforcement, and Safety Act of 2006 introduced requirements for control room management, but the rules—issued by DOT—were not required to be implemented until February 1, 2013, presumably to allow industry time to integrate the necessary technology into their systems.[87] The rules

information sharing between the private sector and the government to ensure greater network security. The bill stems from recent attacks on companies like Target and Sony, and focuses primarily on corporate networks to protect consumer data. H.R. 1560, 114th Cong. (2015).

[78] SCADA IN LIQUID PIPELINES, *supra* note 4, at 3.

[79] WHITE HOUSE, EXEC. OFFICE OF THE PRESIDENT, NSC-63, PRESIDENTIAL DECISION DIRECTIVE: CRITICAL INFRASTRUCTURE PROTECTION (1998) [hereinafter NSC-63], *available at* http://www.fas.org/irp/offdocs/pdd/pdd-63.pdf. A presidential directive (or a presidential decision directive) is a form of executive order that carries the full force of law. Memorandum from the Acting Assistant Attorney General to the Counsel to the President (Jan. 29, 2000), *available at* http://fas.org/irp/offdocs/predirective.html.

[80] *Id.* at 6.

[81] DEP'T OF HOMELAND SEC., HSPD 7, CRITICAL INFRASTRUCTURE IDENTIFICATION, PRIORITIZATION, AND PROTECTION (2003) [hereinafter HSPD 7], *available at* https://www.dhs.gov/homeland-security-presidential-directive-7; *Northeastern Blackout of 2003: Looking Back 10 Years Later*, N.Y. DAILY NEWS (Aug. 14, 2013), http://www.nydailynews.com/new-york/northeast-blackout-2003-back-10-years-gallery-1.1426456.

[82] HSPD 7, *supra* note 81, at 2-3.

[83] DEP'T OF HOMELAND SEC., SCI. & TECH. DIRECTORATE, LOGIIC CYBERSECURITY SYSTEM 1 (2006), *available at* https://www.dhs.gov/sites/default/files/publications/csd-logiic-brochure.pdf. LOGIIC is an acronym for Linking the Oil and Gas Industry to Improve Cybersecurity. *Id.* Developers included DHS, Sandia National Laboratories, Symantec, Honeywell, Chevron, CITGO, BP, and Ergon Refining. *Id.*

[84] IN THE DARK, *supra* note 3, at 19.

[85] *Id.*

[86] Myers, *supra* note 5, at 16.

[87] *Id.* at 18; 49 U.S.C. § 60101 (2012).

require pipeline operators to take into account the National Transportation Safety Board (NTSB) recommendations on SCADA systems.[88]

Legislation on the issue has also been sparse.[89] In April 2011, the White House issued a proposal regarding security measures.[90] Shortly thereafter, the Cybersecurity Act of 2012 passed the House but failed in the Senate, despite reports of recent attacks on pipeline infrastructure.[91] In fact, no major cybersecurity legislation has been enacted since 2002.[92] However, TSA did issue a set of pipeline security guidelines in April 2011 that were developed in conjunction with private industry and that directly addressed the cybersecurity of pipeline SCADA systems.[93] This was the government's first demonstration of effective collaboration with the oil and gas industry to ensure that baseline security measures were in place.

As an apparent stopgap after the failure of the Cybersecurity Act of 2012, the president issued Executive Order 13636 and Presidential Policy Directive 21 on February 12, 2013, requiring the Secretary of Commerce to order NIST to develop a "voluntary information sharing program" with some incentives between the government and private industry.[94] In 2014, the president issued another Executive Order regarding private sector cybersecurity information sharing and ordered the establishment of Information Sharing and Analysis Organizations (ISAOs) to work with the government on its cybersecurity endeavors.[95]

Since the issuance of these executive orders, dozens of members of the oil and gas industry, led by the American Petroleum Institute (API) and the American Gas Association (AGA), have formed two organizations devoted to information sharing—the Oil and Natural Gas Information Sharing and Analysis Center (ONG-ISAC) and the Downstream Natural Gas information Sharing and Analysis Center (DNG-ISAC).[96] These organizations are devoted to communication

[88] Myers, *supra* note 5, at 18, 19.

[89] *DHS Cybersecurity*, *supra* note 77, at 4.

[90] PIPELINE CYBERSECURITY, *supra* note 6, at 1.

[91] *Id.*; Cybersecurity Act of 2012, S. 2105, 112th Cong. (2012); Dylan Walsh, *Cyberstalkers Threaten Pipeline Security*, N.Y. TIMES (Jan. 10, 2013), [hereinafter *Cyberstalkers Threaten Pipeline Security*], http://green.blogs.nytimes.com/2013/01/10/cyberstalkers-threaten-pipeline-security/?_php=true&_type=blogs&_r=2&pagewanted=print.

[92] *DHS Cybersecurity*, *supra* note 77, at 4. The last major cybersecurity legislation enacted was the Homeland Security Act of 2002. 6 U.S.C. § 101 (2002).

[93] TRANSP. SEC. ADMIN., PIPELINE SECURITY GUIDELINES 1-2 (2011), *available at* https://www.tsa.gov/sites/default/files/assets/pdf/Intermodal/tsa_pipeline_sec_guideline_april2011.pdf.

[94] Rob Lever, *White House Mulls Move as Cybersecurity Bill Fails*, YAHOO NEWS (Nov. 16, 2012), http://sg.news.yahoo.com/white-house-mulls-move-cybersecurity-bill-fails-192812872.html; Exec. Order No. 13636, 78 Fed. Reg. 33 (Feb. 19, 2013); WHITE HOUSE, EXEC. OFFICE OF THE PRESIDENT, PPD-21, PRESIDENTIAL POLICY DIRECTIVE: CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE (2013) [hereinafter PPD-21], *available at* https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[95] WHITE HOUSE, EXEC. OFFICE OF THE PRESIDENT, EXECUTIVE ORDER—PROMOTING PRIVATE SECTOR CYBERSECURITY INFORMATION SHARING (2014), *available at* https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.

[96] Collin Eaton, *Oil Industry Forms Clearinghouse for Cyberattack Data*, HOUS. CHRONICLE (June 27, 2014), http://www.houstonchronicle.com/business/energy/article/Oil-industry-forms-clearinghouse-for-cyberattack-5585949.php; *AGA Launches Threat Information Sharing Center for Natural Gas Utilities*, AM. GAS

between oil and gas companies and the government regarding cyber threats and incidents.[97]

III. ANALYSIS

A. DHS Limitations Related to Cybersecurity Efforts

TSA, which monitors oil and gas pipeline cybersecurity, is housed within DHS.[98] Neither may be sufficiently well-equipped to handle cyber threats without industry aid.[99] The President's fiscal year (FY) 2012 budget request for DHS has been criticized as not including a budget for TSA's pipeline security activities.[100] Additionally, in its budget request for FY 2016, TSA only requested $2.9 million for all of its cybersecurity efforts.[101] Staffing and training could also be issues.[102] As of 2013, the Pipeline Security Division (PSD) employed only thirteen employees, funded from TSA's general budget.[103] Moreover, reportedly none of the PSD staff have the specialized computer system expertise needed to monitor extensive cybersecurity activities.[104]

Internal reviews confirm these challenges.[105] In October 2013, DHS's Inspector General conducted an analysis of DHS's efforts to coordinate the activities of federal cyber operations centers, concluding that DHS has insufficient staffing levels that "hinder its ability to provide continuous coverage" in integral mission areas, including pipeline cybersecurity.[106]

Senator Tom Coburn (R-OK) noted in September 2013 that, "[d]espite DHS's growing responsibilities for cybersecurity, the Department is struggling to fulfill its cyber and information technology missions. . . . [T]he Office of the Inspector General found that . . . the Department may not be able to respond effectively in case of an emergency or disaster."[107] Progress has been slow.[108] The

ASS'N (Sept. 9, 2014), https://www.aga.org/news/news-releases/aga-launches-threat-information-sharing-center-natural-gas-utilities.

[97] *AGA Launches Threat Information Sharing Center*, *supra* note 96.

[98] PIPELINE CYBERSECURITY, *supra* note 6, at 5.

[99] PAUL W. PARFOMAK, CONG. RESEARCH SERV., R41536, KEEPING AMERICA'S PIPELINES SAFE AND SECURE: KEY ISSUES FOR CONGRESS 11 (2013), *available at* http://www.fas.org/sgp/crs/homesec/R41536.pdf; PIPELINE CYBERSECURITY, *supra* note 6.

[100] PIPELINE CYBERSECURITY, *supra* note 6, at 5; OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, BUDGET OF THE UNITED STATES GOVERNMENT: FISCAL YEAR 2012 (2011), *available at* http://www.gpo.gov/fdsys/pkg/BUDGET-2012-BUD/pdf/BUDGET-2012-BUD.pdf.

[101] *Written Testimony of TSA Acting Administrator Melvin Carraway for a House Committee on Appropriations, Subcommittee on Homeland Security Hearing on TSA's Fiscal Year 2016 Budget Request*, DEP'T OF HOMELAND SEC. (Mar. 19, 2015), http://www.dhs.gov/news/2015/03/19/written-testimony-tsa-acting-administrator-house-appropriations-subcommittee.

[102] PIPELINE CYBERSECURITY, *supra* note 6, at 6.

[103] *Id.*

[104] *Id.* at 8-9.

[105] DHS' EFFORTS TO COORDINATE, *supra* note 6, at 1.

[106] *Id.*

[107] *See generally 10 Years Later*, *supra* note 6.

[108] *See generally DHS Cybersecurity*, *supra* note 77.

Chairman of the House Committee on Homeland Security noted that there are areas for improvement "across the board" within DHS.[109]

Further, DHS originally struggled to coordinate cybersecurity efforts because of confusion as to which agency—DHS or DOT—was spearheading the process.[110] The two agencies were directed by law to implement a plan together to review the 100 most critical pipeline operators' pipeline security plans and critical facilities, but DHS ultimately carried out the review alone despite its limited resources due to a lack of communication between the agencies that caused continuous delays.[111]

An internal government review determined that while DHS had effectively identified the most critical U.S. oil and gas pipeline systems and had developed a risk model to help address issues with those systems, the models were incomplete.[112] DHS seemed to disregard pipeline systems' risk rankings in considering the priority of system reviews, defeating the purpose of much of the review process.[113] Additionally, even for the highest ranked pipeline systems, the time between the first and second round of reviews ranged from one to seven years, and DHS neither transmitted written post-review to pipeline operators nor followed up with operators to make sure that its recommendations were being implemented.[114] Overall, DHS did not use performance measures and milestones to effectively enhance pipeline SCADA system cybersecurity.[115]

B. Collaboration Between Government and Private Industry

While DHS's efforts alone did not achieve the desired level of cybersecurity in oil and gas pipeline SCADA systems, the collaboration between government and private industry that resulted from the 2013 and 2014 executive orders has made a significant difference in cybersecurity effectiveness.[116] Since 2013, industry members have participated in cybersecurity briefings, security programs, working groups, and risk assessments sponsored by DHS, allowing the government to see firsthand the threats that oil and gas pipeline operators face.[117] The oil and gas industry also collaborated with DHS in writing the Pipeline Security Guidelines released in April 2011, as well as several other sets of

[109] *Id.* at 5.

[110] Memorandum from the Assistant Inspector General for Aviation and Special Program Audits Regarding Actions Needed to Enhance Pipeline Security (May 21, 2008), *available at* https://www.oig.dot.gov/sites/default/files/Pipeline_Security_Report_reissued_AV-2008-53.pdf.

[111] *Id.*

[112] GOV'T ACCOUNTABILITY OFFICE, PIPELINE SECURITY: TSA HAS TAKEN ACTIONS TO HELP STRENGTHEN SECURITY, BUT COULD IMPROVE PRIORITY-SETTING AND ASSESSMENT PROCESSES 17 (2010) [hereinafter TSA ACTIONS], *available at* http://www.gao.gov/new.items/d10867.pdf.

[113] *Id.* at 24, 27.

[114] *Id.* at 26, 39-41.

[115] *Id.* at 48.

[116] Exec. Order No. 13636, *supra* note 94; EXECUTIVE ORDER—PROMOTING PRIVATE SECTOR CYBERSECURITY INFORMATION SHARING, *supra* note 95.

[117] *Cyber Threats and Security Solutions*, 113th Cong. 1, 3-5 (2013), *available at* http://docs.house.gov/meetings/IF/IF00/20130521/100883/HHRG-113-IF00-Wstate-McCurdyD-20130521.pdf (statement of Hon. Dave McCurdy, President and CEO, Am. Gas Ass'n).

voluntary, non-prescriptive guidelines that have begun to shape the cybersecurity landscape for oil and gas pipeline SCADA systems nationwide.[118]

C. The NIST Framework's Attempt to Raise the Bar

1. The Fruits of Information Sharing

Perhaps the largest coordinated cybersecurity effort between government and private industry since the passage of the executive orders is the NIST Framework, released in early 2014.[119] The NIST Framework outlines five "core functions" that private industry should strive to implement, including the identification of weak systems, the development of appropriate safeguards, the detection of cybersecurity breaches, the implementation of an action plan if a breach should occur, and the development of a recovery plan if capabilities are impaired.[120] It then establishes implementation tiers and security "profiles" to help private companies determine where their cybersecurity weaknesses lie, but stops short of fixes.[121] While progress, some criticize the voluntary suggestions as inadequate.[122]

2. Criticisms of Proposed NIST Framework Adoption Incentives

Some have suggested that the NIST Framework is faulty in that there are no incentives for its adoption, and no indicators as to its effectiveness.[123] In order to promote adoption of the NIST Framework, Executive Order 13636 required that DHS, the U.S. Department of Commerce, and the U.S. Department of Treasury draft separate reports suggesting incentives for private corporations.[124] However, the incentives proposed may not be sufficient to overcome the inherent costs.[125] The incentives identified include cybersecurity insurance, grants, process preference, liability limitation, streamline regulations, public recognition, rate recovery for price regulated industries, and cybersecurity research among others.[126]

DHS determined that grants were the most effective incentive but noted that a grant incentive program would require new statutory authority.[127] There were

[118] *Id*. at 4-6.

[119] *See generally* NIST FRAMEWORK, *supra* note 7.

[120] *Id*. at 7.

[121] *Id.* at 9-11; Cynthia Brumfield, *NIST's Latest Cybersecurity Framework Reveals a Lot of Goodwill Amidst Continued Criticism*, CSO (Oct. 24, 2013), http://www.csoonline.com/article/741979/nist-s-latest-cybersecurity-framework-reveals-a-lot-of-goodwill-amidst-continued-criticism?page=2.

[122] Brumfield, *supra* note 121.

[123] James Andrew Lewis, *NIST Cybersecurity Framework*, CTR. FOR STRATEGIC & INT'L STUDIES (Apr. 16, 2014), http://csis.org/publication/nist-cybersecurity-framework.

[124] *Incentives to Support Adoption of the Cybersecurity Framework*, WHITE HOUSE (Aug. 6, 2013), http://www.whitehouse.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework.

[125] DEP'T OF HOMELAND SEC., DHS INCENTIVES STUDY: PRELIMINARY ANALYSIS AND FINDINGS 1, 8 (2013) [hereinafter DHS INCENTIVES STUDY], *available at* http://www.dhs.gov/sites/default/files/publications/niac-mtg-incentive-prelim-analysis-findings-6-21-13.pdf.

[126] *Id.*

[127] *Id.*; DHS INCENTIVES STUDY, *supra* note 125, at 8; DEP'T OF HOMELAND SEC., EXECUTIVE ORDER 13636: IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY INCENTIVES STUDY ANALYTIC REPORT 2, 3 (2013) [hereinafter EXECUTIVE ORDER 13636 INCENTIVES STUDY], *available at*

other state-federal jurisdictional concerns identified as well.[128] The Department of Commerce expressed concern regarding the efficacy of certain ideas brought forth, explicitly stating that tax incentives were not an effective form of incentive for the framework program.[129] The Department of Treasury observed that information sharing was a concern for some stakeholders.[130] The Department of Treasury also expressed concerns about detriments to the federal government in providing liability protection, tax incentives, and cyber insurance.[131] These comments suggest that incentives may not be effective.[132]

D. Alternate Ways to Incentivize Cybersecurity Measures

Although the proposed government incentives may not be influential enough to increase cybersecurity, some believe that there are enough incentives inherent in the NIST Framework (the Framework) to encourage its adoption by private industry.[133] First, the NIST Framework provides a "common language" that has the effect of standardizing the approach to cybersecurity threats.[134] This promotes a more open dialogue about cybersecurity policies and technologies, both internally and externally in conversations with third-party service providers.[135] These discussions with third-party providers are especially important in protecting an oil and gas pipeline's supply chain.[136] Now, a pipeline operator can require that a pipeline SCADA system vendor implement the NIST Framework in its own business practices before any contract or access is granted.[137] Second, the NIST Framework promotes collaboration between private companies, which allows for

https://www.dhs.gov/sites/default/files/publications/dhs-eo13636-analytic-report-cybersecurity-incentives-study.pdf.

[128] EXECUTIVE ORDER 13636 INCENTIVES STUDY, *supra* note 127, at 3.

[129] U.S. DEP'T OF COMMERCE, NAT'L TELECOMM. & INFO. ADMIN., RECOMMENDATIONS TO THE PRESIDENT ON INCENTIVES FOR CRITICAL INFRASTRUCTURE OWNERS AND OPERATORS TO JOIN A VOLUNTARY CYBERSECURITY PROGRAM 3 (2013) [hereinafter RECOMMENDATIONS TO THE PRESIDENT], *available at* http://www.ntia.doc.gov/files/ntia/Commerce_Incentives_Recommendations_Final.pdf; DHS INCENTIVES STUDY, *supra* note 125, at 7-8.

[130] DEP'T OF TREASURY, SUMMARY REPORT TO THE PRESIDENT ON CYBERSECURITY INCENTIVES PURSUANT TO EXECUTIVE ORDER 13636 2, 3, 6 (2013), *available at* http://www.treasury.gov/press-center/Documents/Treasury%20Report%20(Summary)%20to%20the%20President%20on%20Cybersecurity%20Incentives_FINAL.pdf.

[131] *Id.*

[132] *See generally* EXECUTIVE ORDER 13636 INCENTIVES STUDY, *supra* note 127; DHS INCENTIVES STUDY, *supra* note 125; RECOMMENDATIONS TO THE PRESIDENT, *supra* note 129.

[133] Scott J. Shackelford, *Why Ignoring the NIST Framework Could Cost You*, WALL ST. J. (May 2, 2014), http://www.huffingtonpost.com/scott-j-shackelford/why-ignoring-the-nist-fra_b_5244112.html; Yaron Nili, *Understanding the Implementing the NIST Cybersecurity Framework*, HARV. LAW SCH. BLOG (Aug. 25, 2014), http://blogs.law.harvard.edu/corpgov/2014/08/25/understanding-and-implementing-the-nist-cybersecurity-framework/; PWC, WHY YOU SHOULD ADOPT THE NIST CYBERSECURITY FRAMEWORK 5 (2014) [hereinafter WHY YOU SHOULD ADOPT], *available at* http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf.

[134] Nili, *supra* note 133; WHY YOU SHOULD ADOPT, *supra* note 133, at 1, 4.

[135] *Id.*

[136] *Id.*; WHY YOU SHOULD ADOPT, *supra* note 133, at 4.

[137] *Id.*; WHY YOU SHOULD ADOPT, *supra* note 133, at 4, 6.

additional support should an incident occur and enables companies to hold themselves to each other's standards to remain competitive.[138]

Third, and perhaps most importantly, adoption of the NIST Framework may become critical in tort liability.[139] Some speculate that courts may soon determine whether a company's duty has been met in cybersecurity incident situations based on whether or not the company has adopted the NIST Framework.[140] It has been suggested that the NIST Framework could serve "as both a sword and a shield."[141] Failure to implement the NIST Framework could create a presumption of negligence should an incident occur, but adoption of the Framework could also act as a type of safe harbor for companies in attempting to avoid liability.[142] As cyber incidents involving oil and gas pipelines become more widespread and severe, this avoidance of liability could serve as a strong incentive for pipeline operators to adopt the NIST Framework to promote strong cybersecurity measures.

Fourth, the idea that the NIST Framework is a voluntary, "living" document should be attractive to the oil and gas industry, which has largely fought against inflexible regulations and legislation.[143] The NIST Framework has already been revised once since it was first released based on industry responses to a Request for Information, and NIST has released a roadmap indicating that there are still changes to be made and areas to be improved in the near future based on industry suggestions.[144] Finally, DHS provides significant support for entities adopting the NIST Framework through its voluntary Critical Infrastructure Cyber Community, or C3 Program.[145] The program helps private industry to understand the Framework and provides guidance for implementation, outreach for use, and a forum for feedback as to the Framework's effectiveness.[146]

[138] WHY YOU SHOULD ADOPT, *supra* note 133, at 3-4.

[139] Shackelford, *supra* note 133; Nili, *supra* note 133.

[140] Shackelford, *supra* note 133; Nili, *supra* note 133.

[141] Shackelford, *supra* note 133.

[142] Shackelford, *supra* note 133; Nili, *supra* note 133. Some courts have suggested that failure to employ industry standards and industry report recommendations such as the NIST Framework is sufficient for plaintiffs to allege that the company breached its duty to employ reasonable cyber security measures. In some cases, a failure to comply with recommended security measures was enough to establish a triable issue of fact as to whether the duty of care had been breached. SCOTT J. SHACKELFORD, ANDREW A. PROIA, BRENTON MARTELL, & AMANDA N. CRAIG, TOWARD A GLOBAL CYBERSECURITY STANDARD OF CARE? EXPLORING THE IMPLICATIONS OF THE 2014 NIST FRAMEWORK ON SHAPING REASONABLE NATIONAL AND INTERNATIONAL CYBERSECURITY PRACTICES 13-14 (2014), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2446631.

[143] *See generally Cyber Threats and Security Solutions*, *supra* note 117.

[144] NAT'L INST. FOR STANDARDS & TECH., NIST ROADMAP FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (2014), *available at* http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf. These areas include authentication, automated indicator sharing, conformity assessment, the cybersecurity workforce, data analytics, federal agency cybersecurity alignment, international aspects, impacts, and alignment, supply chain risk management, and technical privacy standards. *Id.*

[145] *About the Critical Infrastructure Cyber Community C3 Voluntary Program*, DEP'T OF HOMELAND SEC. (Feb. 12, 2015), http://www.dhs.gov/about-critical-infrastructure-cyber-community-c³-voluntary-program.

[146] *Id.*

E. The ONG-C2M2 as a Buttress to the NIST Framework

From a policy standpoint, although the NIST Framework provides a solid foundation on which to build, this author believes that more should be done to protect oil and gas pipelines—a crucial part of critical infrastructure—from falling into the hands of those with malicious intent.[147] In its update on the framework released in December 2014, NIST admitted that "more could and should be done to raise Framework awareness and use by building on both government and industry-led efforts."[148] NIST also noted that the Framework had led to some confusion regarding terminology, and that there were several updates that needed to be made before the Framework would be fully effective.[149] Most importantly, NIST admitted that feedback from their Request for Information indicated that "closing gaps in cybersecurity risk management identified through the use of the Framework is especially challenging for organizations that do not have existing cybersecurity programs."[150] This challenge results from the limited resources that small- and medium-sized owners and operators of critical infrastructure in the energy sectors have available to devote to cybersecurity efforts.[151] Ultimately, regardless of how many large-scale oil and gas pipeline operators implement the NIST Framework, a system will only be as strong as its weakest link.

That is not to say that the NIST Framework is entirely ineffective. Rather, the NIST Framework needs some added specificity to make its objectives more attainable to smaller oil and gas pipeline entities. In order to achieve this specificity, it would be beneficial to combine the NIST Framework with the ONG-C2M2—developed by DOE and DHS in conjunction with the private sector—to create more tangible goals that align with the NIST Framework's overarching objectives.[152] While the NIST Framework applies to cybersecurity in all industries, the ONG-C2M2 was developed by DOE as the Energy Sector-Specific Agency in order to best include the knowledge and expertise needed to establish an effective model.[153] With the added contributions of energy sector owners and operators, the model gained the specificity and applicability that it needed to become an operational tool.[154] Like the NIST Framework, the ONG-C2M2 remains voluntary, but it outlines both general and tool-specific approaches to implementing the NIST Framework that are better tailored to the cybersecurity needs of oil and gas pipeline operators.[155]

[147] U.S. GOV'T ACCOUNTABILITY OFFICE, CRITICAL INFRASTRUCTURE PROTECTION: CYBERSECURITY GUIDANCE IS AVAILABLE, BUT MORE CAN BE DONE TO PROMOTE ITS USE 32, 34 (2011) [hereinafter CRITICAL INFRASTRUCTURE PROTECTION], *available at* http://www.gao.gov/assets/590/587529.pdf.

[148] NAT'L INST. FOR STANDARDS & TECH., UPDATE ON THE CYBERSECURITY FRAMEWORK 1-2 (2014), *available at* http://www.nist.gov/cyberframework/upload/nist-cybersecurity-framework-update-120514.pdf.

[149] *Id.* at 3-4.

[150] *Id.* at 3.

[151] *Id.* at 4.

[152] *See generally* CYBERSECURITY MODEL, *supra* note 7.

[153] DEP'T OF ENERGY, ENERGY SECTOR CYBERSECURITY FRAMEWORK IMPLEMENTATION GUIDANCE 1 (2015) [hereinafter IMPLEMENTATION GUIDANCE], *available at* http://energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf.

[154] *Id.*

[155] *Id.*

The model is constructed to fortify the weaknesses found in the NIST Framework, including the inability of organizations with less-developed cybersecurity programs to use the NIST Framework due to a lack of resources.[156] By strongly utilizing cybersecurity risk management tools, processes, standards, and guidelines already widely in use throughout the energy sector, the ONG-C2M2 allows businesses to build on the resources that they already have to develop the strongest cybersecurity program possible.[157] The ONG-C2M2 maps to the NIST Framework, so oil and gas pipeline operators can comply with two sets of guidelines with singular efforts.[158] The ONG-C2M2 serves as a "scalable tool" presented at a high level of abstraction so that it can be interpreted and utilized by oil and gas pipeline operators in a way that suits their own types, structures, and sizes.[159] This fixes several of the issues that made the NIST Framework weak as a standalone effort.[160]

While presented at a high level of abstraction so as to allow companies to decide for themselves which measures would be most beneficial to their business practices, the ONG-C2M2 simultaneously provides specificity in that it allows entities to score themselves within each of ten domains, all pertaining to cybersecurity issues.[161] Unlike the NIST Framework, which utilizes a generalized "tier" system, these hard scores allow entities to get a better idea of where exactly their cybersecurity practices lie on a more objective scale.[162] This also allows them to compare their scores to the scores of other entities in the oil and gas sector.[163] After determining where they stand, entities can then set tangible, numeric cybersecurity goals for each of the ten domains—including for their pipeline SCADA systems—allowing the entity to work toward a target profile using manageable, incremental steps.[164]

F. Regulatory or Legislative Requirements as an Additional Fix

Some suggest that formalized regulation or legislation could be helpful by compensating for the NIST Framework's weaknesses.[165] However, opponents of formal regulation in the field of cybersecurity argue that the regulatory approach is not sufficiently flexible to protect against ever-changing threats.[166]

[156] *Id.* at 3.

[157] *Id.* at 5.

[158] IMPLEMENTATION GUIDANCE, *supra* note 153, at 30.

[159] CYBERSECURITY MODEL, *supra* note 7, at 1.

[160] *Id.*

[161] *Id.* at 8. The domains include risk management; asset, change, and configuration management; identity and access management; threat and vulnerability management; situational awareness; information sharing and communications; event and incident response, continuity of operations; supply chain and external dependencies management; workforce management; and cybersecurity program management. *Id.* at 9-10.

[162] *Id.* at 13-15.

[163] *Id.*

[164] CYBERSECURITY MODEL, *supra* note 7, at 18.

[165] EXECUTIVE ORDER 13636 INCENTIVES STUDY, *supra* note 127, at 2-3; DHS INCENTIVES STUDY, *supra* note 125, at 8.

[166] *Cyber Threats and Security Solutions*, *supra* note 117, at 2, 6; *Cyberstalkers Threaten Pipeline Security*, *supra* note 91; *Securing America's Future: The Cybersecurity Act of 2012*, 112th Cong. 38 (2012), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-112shrg73673/html/CHRG-112shrg73673.htm (statement of Tom Ridge on behalf of U.S. Chamber of Commerce). For example, former DHS Secretary Tom Ridge stated,

Additionally, private oil and gas pipeline operators have consistently engaged in effective self-regulation through information sharing and collaboration with government, undermining much of the need for formal measures.[167] Industry members have vocalized that changing this relationship between government and industry to one of "regulator-regulated" would force companies to focus more resources on compliance rather than development of robust cybersecurity programs, hindering implementation of new measures.[168]

There are, nevertheless, some benefits to formal regulation. The mandatory regulations issued by the North American Electric Reliability Corporation (NERC) under the guidance of the Federal Energy Regulatory Commission (FERC) to regulate the cyber security of the electric grid, for example, have forced private entities to increase their cybersecurity standards, ensuring the grid's durability.[169] Compliance is verified, and the FERC is able to conduct the appropriate oversight, review, and approval of all activities.[170] Penalties for non-compliance can be harsh but effective.[171]

Regulation of the pipeline industry lacks symmetry.[172] Private pipeline companies may choose whether or not to follow voluntary guidelines from private sector interest groups.[173] Federal government guidance, including DHS voluntary guidelines for preparing oil and gas critical infrastructure protection plans, have not identified standards.[174]

Canada's example suggests that formal regulation is a possible method for monitoring pipeline cybersecurity.[175] In 2010, after three years of weighing different options and seeking the input of private industry, the Canadian National Energy Board ultimately decided to publish regulatory standards.[176] Policymakers were motivated by 2004 and 2005 security assessments that revealed severe weaknesses in pipeline systems, and decided to issue regulations requiring pipeline operators to devise management plans to meet mandated performance standards.[177] While private industry was still able to participate in the rulemaking

on behalf of the U.S. Chamber of Commerce, that "a regulatory program would likely become highly rigid in practice and thus counterproductive to effective cybersecurity—due in large part to a shift in business' focus from security to compliance." U.S. CHAMBER OF COMMERCE, SECURING AMERICA'S FUTURE: THE CYBERSECURITY ACT OF 2012 (2012).

[167] *Cyber Threats and Security Solutions*, *supra* note 117, at 2, 6.

[168] *Id.* at 6.

[169] CRITICAL INFRASTRUCTURE PROTECTION, *supra* note 147, at 17-18.

[170] *Id.*

[171] *Id.* at 27-28.

[172] *Id.* at 32.

[173] CRITICAL INFRASTRUCTURE PROTECTION, *supra* note 147, at 18-19, 32.

[174] *Id.* at 34.

[175] *See generally Cyberstalkers Threaten Pipeline Security*, *supra* note 91.

[176] *Id.* at 2.

[177] *Id.* The Pipeline Security Management Program required companies to develop, implement, and maintain a program that adequately mitigates the risk of any facilities being protected. The programs implemented should include a policy demonstrating commitment to security, defined roles, responsibilities, and authorities, security training, vulnerability studies, and a process to manage the security of process control and SCADA systems. NAT'L ENERGY BD., NOTICE OF PROPOSED REGULATORY CHANGE 2005-01—PIPELINE SECURITY MANAGEMENT PROGRAMS 3-4 (2005), *available at* https://docs.neb-one.gc.ca/LL-ENG/llisapi.dll/fetch/2000/90463/409054/585323/A1Q8Q7_-

process, the regulatory standards that resulted remained stringent.[178] Although several industry members had commented that the Board should use the program as guidance rather than an enforceable standard, the Board rejected this approach and instead adopted the standard into formal regulations.[179]

The U.S. oil and gas industry is also faced with conflicting guidance from several different public and private organizations.[180] Non-standardized guidance confuses infrastructure owners and detracts from the goal.[181] Policymakers and private industry have called for a more concerted, unified effort on the part of the government to assist the oil and gas industry with establishing consistent cybersecurity standards that will reinforce SCADA systems on pipelines nationwide.[182]

G. Information Sharing Legislation as the Most Effective Solution

While utilizing formal legislation or regulations might be helpful in filling gaps that the voluntary frameworks cannot fill, both the government and the private sector have recognized the importance of not alienating industry in doing so.[183] Therefore, rather than focusing on strict technological standards, any proposed legislation should be more concerned with solidifying the information sharing pathway between the government and the oil and gas industry.[184] DHS's Deputy Secretary Lute stated that "a suite of legislation is necessary to implement the full range of steps needed to build a strong public-private partnership . . . [and] strengthen our critical infrastructure's cybersecurity by further increasing information sharing and promoting the establishment and adoption of standards."[185] Similarly, Gary Hayes, a CenterPoint executive, stated that the most crucial portion of the proposed framework is the intended information sharing process between oil and gas companies and the federal government.[186] Hayes'

_Notice_of_Proposed_Regulatory_Change_2005-01_Pipeline_Security_Management_Programs.pdf?nodeid=585324&vernum=0; NAT'L ENERGY BD., NOTICE OF PROPOSED REGULATORY CHANGE 2009-01—ADOPTION OF CSA Z246.1-09 SECURITY MANAGEMENT FOR THE PETROLEUM AND NATURAL GAS INDUSTRY 1-2 (2009), *available at* https://docs.neb-one.gc.ca/ll-eng/llisapi.dll/fetch/2000/90463/409054/583323/A1Q8F3_%2D_Notice_of_Proposed_Regulatory_Change_2009%2D01_%2D_Adoption_of_CSA_Z246.1%2D09_Security_Management_for_the_Petroleum_and_Natural_Gas_Industry.pdf?nodeid=583324&vernum=-2.

[178] *Cyberstalkers Threaten Pipeline Security*, *supra* note 91; NOTICE OF PROPOSED REGULATORY CHANGE 2005-01, *supra* note 177.

[179] NAT'L ENERGY BD., PROPOSED REGULATORY CHANGE (PRC) 2010-01—ADOPTION OF CSA Z246.1-09 SECURITY MANAGEMENT FOR PETROLEUM AND NATURAL GAS INDUSTRY SYSTEMS 1-2 (2010), *available at* https://docs.neb-one.gc.ca/ll-eng/llisapi.dll/fetch/2000/90463/409054/614444/A1S7H7_%2D_Proposed_Regulatory_Change_%28PRC%29_2010%2D01.pdf?nodeid=614556&vernum=-2.

[180] *SCADA Systems and the Terrorist Threat*, *supra* note 35, at 97.

[181] *Id.*

[182] *Id.*

[183] *DHS Cybersecurity*, *supra* note 77, at 8, 20, 57 (statements of Hon. Bennie G. Thompson, Ranking Member, H. Comm. on Homeland Sec., Jane H. Lute, Deputy Secretary, Dep't of Homeland Sec., and Gary W. Hayes, Chief Information Officer, CenterPoint Energy).

[184] *Cyber Threats and Security Solutions*, *supra* note 117, at 8 (statement of Hon. Dave McCurdy, President and CEO, Am. Gas Ass'n).

[185] *DHS Cybersecurity*, *supra* note 77, at 8, 20 (statements of Hon. Bennie G. Thompson, Ranking Member, H. Comm. on Homeland Sec. and Jane H. Lute, Deputy Secretary, Dep't of Homeland Sec.).

[186] *Id.* at 57 (statement of Gary W. Hayes, Chief Information Officer, CenterPoint Energy).

testimony suggests that the private oil and gas industry welcomes regulation to protect its assets in the sense that the regulation creates a dynamic public-private partnership resulting in industry standardization that is beneficial to all parties.[187] As Hayes analogized, "it is better to see the storm coming, to deal with it than have to react to it after the fact."[188]

Therefore, legislation that streamlines the information sharing process between industry and government and provides information protection mechanisms, safe harbors, and liability protections for oil and gas pipeline owners to encourage disclosure would seem to be the most effective solution to the oil and gas pipeline cybersecurity problem.[189] Congress seems inclined to enact such legislation. The Cyber Threat Sharing Act was introduced in the Senate in February 2015 to establish information sharing processes and procedures and to create liability and proprietary information protections to encourage industry participation, and a similar act, Protecting Cyber Networks Act, was passed by the House of Representatives in April 2015.[190] If information sharing is widespread and oil and gas pipeline operators are protected, they will be much more incentivized to adopt the NIST Framework, utilize the ONG-C2M2, and engage in ISACs.[191]

President Obama supported these legislative initiatives at the White House Summit on Cybersecurity and Consumer Protection in February 2015, where he encouraged cybersecurity legislation that enhances collaboration and information sharing by providing "targeted" liability protection for any private entities that share information with the government.[192] President Obama also proposed formalizing the Information Sharing and Analysis Organizations of which the oil and natural gas industries are already members to allow them greater security in their disclosures.[193] If enacted, this proposed legislation could create the formalization that is needed to encourage information sharing and the adoption of voluntary frameworks without creating a rigid regulatory scheme that undermines cybersecurity development.[194]

IV. CONCLUSION

The author believes that the threat of large-scale cyber attacks on the nation's pipeline SCADA systems is increasing. However, despite the growing threat of attack to the oil and gas industry, pipeline SCADA systems remain wanting in the area of cybersecurity. Numerous system vulnerabilities open pathways for

[187] *DHS Cybersecurity*, *supra* note 77, at 62 (statement of Gary W. Hayes, Chief Information Officer, CenterPoint Energy).

[188] *Id.* at 71.

[189] *Cyber Threats and Security Solutions*, *supra* note 117, at 8 (statement of Hon. Dave McCurdy, President and CEO, Am. Gas Ass'n).

[190] S. 456, 114th Cong. (as introduced in the Senate, Feb. 11, 2015); H.R. 1560, 114th Cong. (2015).

[191] *Cyber Threats and Security Solutions*, *supra* note 117, at 11-12 (statement of Hon. Dave McCurdy, President and CEO, Am. Gas Ass'n).

[192] Press Release, White House, Fact Sheet: White House Summit on Cybersecurity and Consumer Protection (Feb. 13, 2015), https://www.whitehouse.gov/the-press-office/2015/02/13/fact-sheet-white-house-summit-cybersecurity-and-consumer-protection.

[193] *Id.*

[194] SECURING AMERICA'S FUTURE, *supra* note 166.

malicious attackers to wreak havoc while the government remains slow-moving in legislating on the issue.

However, the NIST Framework and the ONG-C2M2 combine to lay a strong foundation for the development of increased cybersecurity in the oil and gas pipeline sectors. With increased information sharing between the private sector and the government and specific, numeric objectives to work toward in developing cybersecurity programs for pipeline SCADA systems, the voluntary measures currently in place might prove effective in protecting systems nationwide. These voluntary measures could be made even stronger by the introduction and passage of formal legislation streamlining the information sharing process and providing liability and privacy protection for oil and gas pipeline owners, which would further incentivize industry participation.

Rather than wait for an attack to occur to spark implementation of cyber security measures in SCADA systems, the government—working alongside private industry—should be proactive, anticipating the storm to come. Oil and gas resources should be more protected from destruction through the best voluntary cybersecurity programs possible, thereby guarding the American people from the consequences that might result from a large-scale pipeline cyber attack. To pretend that a devastating attack is not forthcoming because one has not yet succeeded is to regress to a mindset that was only practical before the advent of terrorist groups, the rise of modern technology, and the popularity of anonymous cyber activity.

Hillary Hellmann[*]

[*] J.D. May 2015, The University of Tulsa College of Law; B.A. Political Science and Spanish, Certificate in International Studies, The University of Tulsa. Prior to law school, Ms. Hellmann completed eighteen hours of graduate course work in computer science and cybersecurity and has conducted multiple internships within the U.S. intelligence community.