PREVENTING CYBERGEDDON: HOW COMPREHENSIVE REGULATION CAN HELP PROTECT AMERICAN CRITICAL INFRASTRUCTURE SYSTEMS FROM CYBERATTACKS

By: Graves Peeler[*]

I. INTRODUCTION

On May 7, 2021, hackers believed to be working out of Russia or Eastern Europe attacked the Colonial Pipeline Company, deploying ransomware against the pipeline company's business systems which control the distribution of oil and gas through its pipelines along the southeastern part of the United States.[1] Luckily for Colonial and the population of the southeastern states, this was a ransomware attack and not an act of sabotage; the hackers only held the pipeline controls

* University of Houston Law Center, Juris Doctor Candidate, 2023. Thank you, Board 23, for your diligence and thoughtfulness in editing this article. Thank you to my parents and siblings, who have always believed in me. Finally, special thanks to my fiancé, Julia, for being my biggest supporter; your love and support has helped me excel in ways I couldn't have imagined.

1. *Colonial Pipeline Cyberattack Highlights Need for Better Federal and Private-Sector Preparedness*, U.S. GOV'T ACCOUNTABILITY OFF. (May 18, 2021), https://www.gao.gov/blog/colonial-pipeline-cyberattack-highlights-need-better-federal-and-private-sector-preparedness-infographic [hereinafter *Colonial Pipeline Cyberattack*]; David E. Sanger & Nicole Perlroth, *F.B.I. Identifies Group Behind Pipeline Hack*, THE N.Y. TIMES (May 10, 2021), https://www.nytimes.com/2021/05/10/us/politics/pipeline-hack-darkside.html.

hostage for money as opposed to causing physical, lasting harm to the infrastructure system.[2] Although Colonial's critical infrastructure was untouched, it cost the company upwards of $5 million in ransom payments to the cyber-terrorist group.[3] More importantly, the United States saw the average national retail gas price rise above $3 a gallon for the first time in years.[4]

Attacks on critical American infrastructure sectors like the Colonial Pipeline attack are more commonplace in today's world, with attempted attacks on operational technology assets and industrial control systems increasing by two thousand percent between 2018 and 2020.[5] In March of 2018, the Department of Homeland Security reported that hackers inside of Russia hacked their way into machines in nuclear power plants in the United States gaining access to critical control systems.[6] An attack of such magnitude could cripple the United States financially, politically, and militarily.

Nation-states have done more than make idle threats to disrupt the American power grid and other critical infrastructure systems. In 2014, the United States indicted five Chinese military hackers for hacking into several private American companies, including a nuclear power plant products and services company, a specialty metals and components supplier for the aerospace and defense industries, and a major U.S. steel producer.[7] Admiral Michael Rogers, the then head of the National Security Agency, testified before Congress that countries like China now have the ability to launch a cyberattack that could shut down the entire U.S. power grid, and that it is only a matter of when, not if, we are going to see something traumatic occur.[8]

---

2. *Colonial Pipeline Cyberattack*, *supra* note 1.

3. *Id.*; William Turton, Michael Riley & Jennifer Jacobs, *Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom*, BLOOMBERG (May 13, 2021, 9:15 AM), https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom.

4. Grace Dean, *Drivers face $3 gas prices after the Colonial Pipeline cyberattack, and some gas stations have run out completely,* BUS. INSIDER (May 11, 2021, 7:51 AM), https://www.businessinsider.com/gas-prices-colonial-pipeline-cyberattack-fuel-east-coast-2021-5.

5. David Bisson, *Amateur Critical Infrastructure Attacks Growing in Frequency Relative Severity*, SECURITYINTELLIGENCE (July 5, 2021), https://securityintelligence.com/news/amateur-critical-infrastructure-attacks-growing-frequency-severity/.

6. Nicole Perlroth & David E. Sanger, *Cyberattacks Put Russian Fingers on the Switch at Power Plants, U.S. Says,* THE N.Y. TIMES (Mar. 15, 2018), https://www.nytimes.com/2018/03/15/us/politics/russia-cyberattacks.html.

7. *See* Press Release, U.S. Dep't of Just., *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage* (May 19, 2014).

8. *Cybersecurity Threats: Hearing Before H. Select Intel. Comm.*, C-SPAN (Nov. 20, 2014) (statement of Admiral Michael Rogers, NSA Director and U.S. Cyber Command Commander), https://www.c-span.org/video/?322853-1/hearing-cybersecurity-threats.

While it is almost certain that American military forces are responding proportionately to these attacks by foreign adversaries,[9] America is hindered by the fact that the private sector in the country owns 85 percent of the nation's critical infrastructure systems, something authoritarian countries like Russia and China do not have to contend for in defending cyber infrastructure.[10] This places the protection of critical infrastructure facilities like nuclear power plants, energy pipelines, hydroelectric dams, and healthcare infrastructure out of the government's direct control, creating a massive national security problem for the federal government.[11] In America, conflicts arise between regulations protecting the public interest and private companies' need for profit maximization. Often, massive gaps are created between what companies should be doing to better protect against threats like cyberattacks and what they are actually doing.[12]

This paper will argue that because the private sector does not have much incentive to spend the funds on improving and creating preventative cybersecurity systems, the federal government must create a clear set of regulations that motivate the private sector to improve cyber defenses and take preventative measures against attacks, thus improving the nation's overall defensive capabilities against foreign cyberattacks. It will also provide a better framework by which the courts' system can hold private companies accountable when they fail to protect critical infrastructure, like pipelines and power plants, from being sabotaged or held for ransom.

Part II of this paper will outline the history and scope of the cyber threats facing American critical infrastructure and the lack of response from the private sector. Understanding how this threat has evolved since the start of the millennium will help determine how the private sector and government will have to work together to create a better cybersecurity defense strategy that is more proactive than reactive.[13]

Part III will discuss and evaluate current government attempts at improving the private sector's cyber defenses in critical infrastructure. While the current federal system's attempt at regulating the cyber industry is quite messy, proposed laws could have a significant impact,

---

9. CNET, *How the US hacks other countries,* TECHREPUBLIC (Apr. 10, 2020) (interview by Dan Patterson, Senior Producer at CNET, with Robert Lee, Founder & CEO of Dragos, Inc.), https://www.techrepublic.com/article/how-the-us-hacks-other-countries/.

10. U.S. GOV'T ACCOUNTABILITY OFF., GAO-07-39, CRITICAL INFRASTRUCTURE PROTECTION: PROGRESS COORDINATING GOVERNMENT AND PRIVATE SECTOR EFFORTS VARIES BY SECTORS' CHARACTERISTICS 1 (2006).

11. *See id.* at 1, 36.

12. *See* Robert Kenneth Palmer, *Critical Infrastructure: Legislative Factors for Preventing a "Cyber-Pearl Harbor"*, 18 VA. J.L. & TECH. 289, 335 (2014).

13. *Id*. at 293-95, 297-98.

both good and bad, like the Cyber Incident Reporting for Critical Infrastructure Act of 2021.[14]

Part IV will conclude with a discussion of how proposed regulations, like mandatory disclosure of cybersecurity incidents, will affect how courts might hold critical infrastructure companies accountable after a cyberattack. Courts have been trying to find a standard to hold companies accountable when they fail to stop cyberattacks, especially when there were known vulnerabilities in their systems[15], and a uniform set of rules and regulations might make the court's job easier.

So far, courts hold companies to what a reasonable and prudent business would have done in a similar situation, but this becomes foggy when multiple companies are involved in a data breach with each pointing the finger at the other.[16] Uniform federal regulation could alleviate the initial burden on courts to sift through complex cybersecurity matters in determining liability if there were a federal agency that was already monitoring the situation closely.

II. UNDERSTANDING THE THREAT

President Barack Obama characterized cybersecurity threats to critical infrastructure as "one of the most serious national security challenges" confronting the United States.[17] He believed that enemies of the United States possess the "ability to sabotage our power grid, our financial institutions, [and] our air traffic control systems."[18]

These risks are particularly worrisome for critical infrastructure systems such as power plants, power grids, chemical factories, bridges and highways, financial institutions, transportation networks, and communications networks.[19] In 2013, President Obama released a presidential policy directive which highlighted sixteen industries

---

14. Cyber Incident Reporting for Critical Infrastructure Act of 2021, 117th Cong. (2021)(creating a federal agency responsible for overseeing critical infrastructure and requiring entities that own or operate critical infrastructure to report cybersecurity incidents to this agency).

15. In re Equifax Inc. Sec. Litig., 357 F.Supp.3d 1189, 1219-20, 1234, 1236 (N.D. Ga. 2019)(dismissing most of Equifax's corporate officers from the Amended Complaint for lack of particularized facts establishing the scienter requirement, despite a finding that false or misleading statements were made as to the adequacy of Equifax's data security).

16. *See infra* Part IV; *see also* John Reed Stark, *Is Amazon Liable for the Capital One Hack?*, LINKEDIN: PULSE (Aug. 8, 2019), https://www.linkedin.com/pulse/amazon-liable-capital-one-hack-john-reed-stark/?trackingId=dKIReSKmQmmaagpg4hn91w%3D%3D.

17. Exec. Order No. 13,636, 3 C.F.R. § 1 (2013).

18. Press Release, The White House, President Barack Obama's State of the Union Address (Feb. 12, 2013), http://www.whitehouse.gov/ the-press-office/2013/02/12/remarks-presidentstate-union-address.

19. *The Cybersecurity Partnership Between the Private Sector and Our Government: Protecting Our National and Economic Security: J. Hearing Before the S. Comm. on Commerce, Sci., & Transp. and S. Comm. on Homeland Sec. & Governmental Affairs*, 113th Cong. 3–4 (2013) (statement of Janet Napolitano, Sec'y, U.S. Dep't of Homeland Security).

considered to be part of American critical infrastructure: chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial bases, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors and materials, transportation systems, and water and wastewater systems.[20]

One of the more recent attacks seen on U.S. soil was the SolarWinds hack, which happened sometime in early 2020.[21] SolarWinds' Orion network management system keeps a watchful eye on all the various components of a company's network.[22] Microsoft, Intel, Cisco, the United States Treasury, the Department of Justice, the Department of Energy, and the Pentagon were some of the around one hundred companies and agencies affected by the attack.[23] The Russian-based hack even infiltrated the Cybersecurity and Infrastructure Security Agency (CISA).[24] The extent of damage is still unknown, but some experts worry that this was just an introduction for the Foreign Intelligence Service of the Russian Federation into the U.S.'s critical infrastructure network to lay the groundwork for something far more devastating in the future.[25]

There were signs early on that suspicious activity was occurring on SolarWinds's clients' computers.[26] An employee for a D.C.-based cybersecurity company spotted suspicious activity in a client's computer and addressed the problem but did not report it to SolarWinds or any government agency because he did not have enough detailed information.[27]

Palo Alto Networks, another cybersecurity firm, did notify SolarWinds of a problem in their Orion software, but SolarWinds failed to find the problem after three months.[28] SolarWinds' CEO admitted that despite working to "pick up the problem and walk it back," the issue was "closed" before identifying the origin of the hack.[29] A former member of the SolarWinds security team left the company in 2017, stating that

---

20. THE WHITE HOUSE, *Presidential Policy Directive/PPD-21: Critical Infrastructure Security and Resilience*, 1, 10–11 (Feb. 19, 2013).

21. Dina Temple-Raston, *A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Hack*, NPR (Apr. 16, 2021, 10:05 AM), https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.

22. *Id*.

23. *Id*.

24. *Id*.

25. *Weathering the Storm: The Role of Private Tech in the Solarwinds Breach and Ongoing Campaign: J. Hearing Before the H. Comm. on Oversight & Reform and the H. Comm. on Homeland Sec.*, 117th Cong. 1-4, 16-17, 56, 67 (2021) (statements of Hon. Carolyn B. Maloney, Rep. N.Y. 12th Dist.; Hon. James Comer, Rep. Ky. 1st Dist.; Kevin Mandia, CEO, FireEyes, Inc.).

26. Temple-Raston, *supra* note 21.

27. *Id*.

28. *Id*.

29. *Id*.

SolarWinds' management did not want to spend the necessary funds on security.[30]

The SolarWinds attack shows the self-inflicted vulnerability corporations are willing to subject themselves to in order to maximize profit.[31] For SolarWinds, it did not want to spend the funds necessary on preventative cybersecurity systems, nor did it want to spend the time and labor collecting data that would have helped fix the problems caused by the hackers.[32]

In 2017, Wolf Creek Nuclear Operating Corporation reported that hackers wrote highly targeted phishing emails that allowed them to access the critical industrial control systems of the power plant.[33] While there was no operational damage, experts have warned that hackers could use remote access to cause physical destruction of nuclear plants.[34]

Manufacturers, nuclear plant operators, and pipeline operators use supervisory control and data acquisition systems (SCADA) to monitor variables like pressure and flow rates through pipelines, making them targets for malicious hacks.[35] Security specialists have warned that hackers who can access SCADA systems might remotely cause destruction to critical infrastructure systems. This could cause entire parts of the electrical grid to shut off.[36] After attacks, companies like SolarWinds and Wolf Creek are under no obligation to report the cyber incidents to any federal agency; all current reporting programs are voluntary.[37]

A lack of a reporting system that could disclose how, when, and why a critical infrastructure company was targeted is the main reason why companies fail to take adequate measures in preventing the next attack.[38] Many experts believe that companies would rather hide their failures as best they can to appease shareholders, keep stock prices from

---

30. *See* Temple-Raston, *supra* note 21.

31. Ashley Lukehart, *U.S. Critical Infrastructure: Addressing Cyber Threats and the Importance of Prevention*, TRIPWIRE (May 31, 2021), https://www.tripwire.com/state-of-security/featured/critical-infrastructure-addressing-cyber-threats-importance-of-prevention/.

32. *See* Temple-Raston, *supra* note 21.

33. Nicole Perlroth, *Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I Say*, THE N.Y. TIMES (July 6, 2017), https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html.

34. *Id*.

35. *Id*.

36. *Id.*

37. *See* Cyber Incident Reporting for Critical Infrastructure Act of 2021, H.R. 5440, 117th Cong. § 220A (2021) (amending 6 U.S.C 651 et seq.) (proposing mandatory reporting requirements for cybersecurity incidents involving entities that operate critical infrastructure).

38. NAT'L INFRASTRUCTURE ADVISORY COUNCIL, SECURING CYBER ASSETS: ADDRESSING URGENT CYBER THREATS TO CRITICAL INFRASTRUCTURE 8-9 (2017).

plummeting, and avoid panicked consumers.[39] Most importantly, companies want to avoid what will likely be substantial expenses required in upkeeping security systems.[40]

Cybersecurity problems are best analogized with pollution in the energy sector.[41] Both of these fields deal with negative externalities, so, just as companies underinvest in pollution controls because some of their pollution costs are borne by those downwind, companies "also tend to underinvest in cybersecurity systems because some of the costs of intrusion are externalized to others."[42]

Private sector leaders continue to fight any mandatory regulation of critical infrastructure security systems, but the evidence tends to show that the market has failed to properly regulate itself, much like energy firms and environmental pollution, which calls for government intervention.[43] Attacks will continue to increase as companies are more willing to pay off ransoms to hackers but refuse to share any information about attacks or update security systems with preventative software because it would hurt their revenue or earnings per share at the end of the quarter.[44] As former Security and Exchange Commission Chairman Christopher Cox stated, "voluntary regulation of cybersecurity does not work."[45]

Companies need to be regulated and mandated to take certain actions to protect their critical infrastructure systems. In order to incentivize and create stronger protection from crippling cyberattacks, the federal government must step in and ensure that these companies are taking the necessary steps to protect critical infrastructure systems.[46] These steps can include mandatory disclosure systems, periodic audits of security systems, and required types of minimum security systems depending on the industry.[47] All of these may help not only respond to attacks adequately but also prevent future attacks. A single regulatory agency will be able to collect data from across the

---

39. Espellman, *20% of Security Professionals Say their Company has Hidden or Covered Up a Breach*, IT GOVERNANCE USA BLOG (May 18, 2015), https://www.itgovernanceusa.com/blog/20-of-security-professionals-say-their-company-has-hidden-or-covered-up-a-breach.

40. Danielle Warner, *From Bombs and Bullets to Botnets and Bytes: Cyber War and the Need for a Federal Cybersecurity Agency*, 85 S. CAL. L. REV. Postscript 1, 16-17 (2012).

41. Amitai Etzioni, The Private Sector: A Reluctant Partner in Cybersecurity, GEO. WASH. UNIV. INST. FOR COMMUNITARIAN POL'Y STUD. (Dec. 2014), https://icps.gwu.edu/private-sector-reluctant-partner-cybersecurity#_ednref16.

42. *Id*.

43. *Id*.

44. *Cybereason: Paying ransoms leads to more ransomware attacks*, TECHTARGET (June 7, 2022), https://www.techtarget.com/searchsecurity/news/252521164/Cybereason-Paying-ransoms-leads-to-more-ransomware-attacks; Etzioni, *supra* note 41.

45. Etzioni, *supra* note 41.

46. *See* Nathan Alexander Sales, *Regulating Cyber Security*, 107 NORTHWESTERN U. L. REV. 1503, 1555-56 (2013).

47. *Id*. at 1556.

critical infrastructure sector and analyze how attacks are planned and executed. The agency would see who is being targeted and what kinds of technologies are being implemented or could be implemented in the attacks.

There will likely need to be something akin to the SEC or EPA, where a single agency is in charge of monitoring critical infrastructure firms and helping prevent and respond to attacks on their systems. Of course, companies will drag their feet because no one likes being regulated by the federal government. However, all financial motives tend to point against companies taking preventative actions on their own when it comes to cybersecurity.[48]

While the disclosure of information related to cybersecurity will be similar to what the SEC requires of financial information for publicly traded companies, this agency should be completely private and secure. Companies will be more willing to comply if they know that their information and technology are protected.[49] However, while centrality is a huge benefit, storing lots of extremely sensitive and valuable information will make the agency a prime target for hackers.[50]

III. A LOOK AT THE CURRENT FEDERAL RESPONSE TO INCREASING CYBERATTACKS ON CRITICAL INFRASTRUCTURE

Companies operating critical infrastructure systems are at risk of being targeted if they have not already been subject to an attempted or successful hack from malicious foreign actors.[51] On August 27, 2021, with SolarWinds and Colonial Pipeline hacks fresh on the minds of most Americans, the U.S. House of Representatives Homeland Security Committee released a draft bill that would update the Homeland Security Act of 2002.[52] The proposed bill would establish a Cyber Incident Review Office within the CISA and publish a rule that would outline procedures for reporting cybersecurity incidents.[53] The

48. Alexander Botting, *Cybersecurity in the private sector – playing catch-up*, THE HILL (May 13, 2014, 9:00 AM), https://thehill.com/blogs/congress-blog/technology/205883-cybersecurity-in-the-private-sector-playing-catch-up.

49. Brad Williams, *Mandatory Cyber Reporting Within 24 Hours: Sen. Warner Bill*, BREAKING DEFENSE (June 21, 2021, 5:12 PM), https://breakingdefense.com/2021/06/mandatory-cyber-incident-reporting-within-24-hours-sen-warner-bill/.

50. Babur Khan, *Why are Government Agencies So Vulnerable to Hacking?*, A10 BLOG (Oct. 20, 2020), https://www.a10networks.com/blog/why-are-government-agencies-so-vulnerable-to-hacking/.

51. *See* Tadas Limba, et al., *Cybersecurity Management Model for Critical Infrastructure*, 4 INT'L. J. ENTRPRENUERSHIP AND SUSTAINABILITY ISSUES 559, 561-63 (Apr. 20, 2017) (stating that critical infrastructure is targeted because entities employ established commercial solutions that have known vulnerabilities).

52. Charlie Moskowitz, *What is Cyber Incident Reporting for Critical Infrastructure Act of 2021?*, SECURITYSCORECARD (Sept. 28, 2021), https://securityscorecard.com/blog/what-is-cyber-incident-reporting-for-critical-infrastructure-act-of-2021.

53. *Id.*

committee believes that "[c]reating standardized reporting requirements and a set of processes overseen by a single agency office will help centralize information and ensure consistent responses to attacks."[54] The legislation will create, within the CIRA, a new Cyber Incident Review Office (CIRO).[55]

A. Defining Covered Entities

The CIRO will serve as the point of contact for all information collecting regarding covered cybersecurity incidents in an effort by the federal government to centralize and standardize where and how reporting on cyberattacks on critical infrastructure systems is to occur.[56] The CIRO will receive reports of cybersecurity incidents and review the reports in order to disseminate the information to relevant intelligence agencies, other critical infrastructure companies, and cybersecurity firms that could be affected by the attack.[57] If the CIRO determines that a company is a covered entity, the company is required to submit reports of cybersecurity incidents to them.[58]

The Secretary of the CISA, in consultation with other heads of federal departments and agencies, determines which critical infrastructure firms will be required to disclose cyber incidents to the CIRO.[59] When making a determination, the Secretary must consider:

the consequences that disruption to or compromise of such an entity could cause to national security, economic security, or public health and safety; (B) the likelihood that such an entity may be targeted by a malicious cyber actor, including a foreign country; (C) the extent to which damage, disruption, or unauthorized access to such [an] entity will disrupt the reliable operation of other critical infrastructure assets; and (D) the extent to which an entity or sector is subject to existing regulatory requirements to report cybersecurity incidents . . . .[60]

This bill is still in committee, so there has not been a list or specific categories of what companies will be required to report cybersecurity incidents. However, the CISA has highlighted sixteen critical infrastructure sectors: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture;

---

54. *Id.*

55. Cyber Incident Reporting for Critical Infrastructure Act of 2021, H.R. 5440, 117th Cong. (2021).

56. Moskowitz, *supra* note 53.

57. Cyber Incident Reporting for Critical Infrastructure Act of 2021, § 2220A(c).

58. § 2220A(d)(1)(A).

59. §§ 2220A(a), (d)(defining covered entity as an entity that owns or operates critical infrastructure that satisfies the definition established by the Director in the interim final rule and final rule issued pursuant to section 2220A).

60. *Id.* at sec. 2(a) § 2220A(d)(2).

government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.[61]

Across all these different sectors, there is one common feature when it comes to the technology implanted in the private companies occupying these spaces—life critical embedded systems.[62] Life critical embedded systems are systems that, if hacked and destroyed or forced to fail, will result in death or serious harm to people, large financial losses, or loss or severe damage to critical equipment.[63] These are things like SCADAs or industrial control systems that regulate power entering a grid or the coolant flowing through a nuclear reactor.[64]

Any private company that operates in a critical infrastructure sector using a type of life critical embedded system should fall under "covered entities" and be required to report cybersecurity incidents. As the proposed legislation currently stands, the term "covered entity" means any "entity that owns or operates critical infrastructure that satisfies the definition established by the Director."[65]

Furthermore, since some critical infrastructure companies outsource their cybersecurity systems to large cybersecurity firms,[66] any cybersecurity firm whose client operates critical infrastructure and has a life critical embedded system should also be subject to reporting to CIRO. Companies who operate or monitor critical infrastructure facilities that employ hardware or software that, if hacked and compromised, could cause substantial harm should be considered covered entities subject to reporting requirements. This should give the CIRO access to data in its incident reports from all entities involved allowing a comprehensive view of the incident. For effective response and prevention, it is vital to know who was affected, who needs to be notified, what is the best response, what other companies might be future targets, and what bottlenecks in the cyber supply chain require monitoring going forward to prevent a similar attack.[67]

B. Determining Which Cybersecurity Incidents Require

---

61. *Critical Infrastructure Sectors*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/critical-infrastructure-sectors (last visited Oct. 21, 2020).

62. *Security Tenets for Life Critical Embedded Systems*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, (Nov. 20, 2015), https://www.cisa.gov/sites/default/files/publications/security-tenets-lces-paper-11-20-15-508.pdf.

63. *Id*.

64. *Id*.

65. Cyber Incident Reporting Act of 2021, S. 2875, 117th Cong. § 2230(b)(3) (2021).

66. *See The Cybersecurity Risks of Outsourcing to Third Parties*, IDENTITY MGMT. INST. (Sept. 29, 2020), https://identitymanagementinstitute.org/the-cybersecurity-risks-of-outsourcing-to-third-parties/.

67. *See* Traci Spencer, *How to Respond to a Cyber Attack*, NAT'L INST. OF STANDARDS AND TECH.: MFG. INNOVATION BLOG (Nov. 14, 2019), https://www.nist.gov/blogs/manufacturing-innovation-blog/how-respond-cyber-attack.

Disclosure And How They Should Be Disclosed

The Secretary would determine what type of cybersecurity incidents will be subjected to the reporting requirements.[68] The Act would require, at a minimum, a rule that defines a covered cybersecurity incident to be an incident where there was unauthorized access to a network, information system, industrial control system, or any other operational system.[69] At the other end of the spectrum are significant cybersecurity incidents where a single hack or a group of related hacks is likely to result in harm to people, the economy, civil liberties, or public health.[70] This broad definition of cybersecurity incident will cover everything from suspicious logins and phishing emails like those used to hack into Colonial Pipeline,[71] to malware attacks on nuclear powerplants.

For the CIRO to be effective, the breadth of cyber problems falling under covered incidents should be as broad as possible. Often, like in the Colonial Pipeline hack, large-scale attacks start with the smallest points of intrusion.[72] The key to successful regulation and prevention of cyberattacks will be the full and timely disclosure of any suspicious activity. Much like how reporting companies must submit standardized 10-K Forms to the SEC for financial disclosure regulations,[73] an agency like the CIRO should create standardized reporting forms that creates no wiggle room for companies to leave out key cyber incidents. If the CIRO, or some other agency like it in the future, wants to be serious about curbing cyberattacks, it should require standardized disclosure and make clear what requires disclosure. This will make it easier to report and cheaper to look for these certain incidents.

Companies, like SolarWinds, that experience problems with cyber security drag their feet when it comes to telling the public about such incidents because of the negative publicity, which in turn hurts their business.[74] Financially, there is not much incentive to report any cyber

---

68. Cyber Incident Reporting for Critical Infrastructure Act of 2021, sec. 2, § 2220A(d)(2).

69. *Id*. at § 2220A(d)(4)(B).

70. *Id*. at § 2220A(a)(14).

71. *See* Abhishek Gharat, *Colonial Pipeline Cyber Incident Used as Phishing Bait in Help Desk Scam*, CYBER SEC. ASS'N (Jun. 11, 2021), https://cybersecurityassociation.co/colonial-pipeline-cyber-incident-used-as-phishing-bait-in-help-desk-scam/.

72. *See id*.

73. *See* Sec. and Exch. Comm'n, *Exch. Act Reporting and Registration* (Apr. 28, 2022), https://www.sec.gov/education/smallbusiness/goingpublic/exchangeactreporting (stating that SEC rules require a filing of a 10-K form annually).

74. *See* Russell Brandom, *SolarWinds hides list of high-profile customers after devastating hack*, THE VERGE (Dec. 15, 2020, 11:05 AM), https://www.theverge.com/2020/12/15/22176053/solarwinds-hack-client-list-russia-orion-it-compromised.

incidents, especially seemingly "minor" intrusions.[75] To combat negative financial incentives, a regulatory body like the CISA needs to have a specific list of what information regarding a company's cybersecurity system must be reported to the CIRO. If the CISA allows companies to determine what the companies report, financial incentives will drive companies to hide cyber incidents that are not obvious.[76] This will diminish the agency's ability to properly regulate and prevent attacks because it will have less data to formulate responses and preventative measures. Furthermore, it might miss out on some new form of a cyberattack that calls for new defensive measures to be created or fail to warn other firms which might be attacked next.

The Director must also establish the timeframe in which the covered entity must report the attack or threat to the CIRO.[77] Relevant factors to be considered are things like the nature of the attack, the severity, and the complexity of the attack.[78] However, the Act does not allow the timeframe for reporting to be earlier than 72 hours after a covered entity reasonably believes that an incident has occurred.[79] The quicker an attack is reported, the faster the CIRO will be able to assess the severity and extent of the attack so it can notify other companies who might be affected. The goal of an agency like the CIRO should be to assist in remedial efforts as soon as possible. The quicker reporting is required, the faster data is collected and disseminated to the public, who can then act on that information to prevent similar attacks.

While the 72-hour reporting window is better than the previous reporting system, which was completely voluntary and barely used, an even more immediate reporting system, like the EPA's oil discharge reporting requirements, would be better.[80] The EPA's discharge reporting system requires any person in charge of an offshore or onshore facility to report hazardous spills immediately to the EPA because such incidents are extremely time-sensitive.[81]

---

75. Maya Villasenor, *Consumer-facing Companies Still Have Few Incentives to Stop Data Breaches, and That's a National Security Concern*, COUNCIL ON FOREIGN RELS. (Oct. 26, 2021, 1:11 PM), https://www.cfr.org/blog/consumer-facing-companies-still-have-few-incentives-stop-data-breaches-and-thats-national.

76. *See* Dan Swinhoe, *Why Businesses Don't Report Cybercrimes to Law Enforcement*, CSO (May 30, 2019, 3:00 AM), https://www.csoonline.com/article/3398700/why-businesses-don-t-report-cybercrimes-to-law-enforcement.html.

77. Cyber Incident Reporting for Critical Infrastructure Act of 2021, H.R. 5440, 117th Cong. § 2220A(5)(A)(i) (2021).

78. *Id*.

79. *Id*.

80. *Spill Reporting Matrix*, RETAIL COMPLIANCE CTR. (Jan. 1, 2020), https://www.rila.org/retail-compliance-center/spill-reporting#:~:text=If%20a%20hazardous%20substance%20is,requirements%20must%20also%20be%20followed.

81. *See When are You Required to Report an Oil Spill and Hazardous Substance Release?*, EPA, https://www.epa.gov/emergency-response/when-are-you-required-report-oil-spill-and-hazardous-substance-release (Aug. 12, 2022).

Much like how remedial efforts in an oil spill are contingent on fast responses, an agency like the CISA will find success if incidents are reported immediately. For example, had SolarWinds been required to report its breach immediately as opposed to waiting three months, an agency like the CISA could have stepped in. That agency could have assessed the situation, notified the affected parties, and started to figure out exactly what the problem was, how to fix it, and how to stop it from happening again.

C. Enforcement Against Inaction

While a new regulatory body is needed, it will not have much, if any, effect on how private infrastructure firms handle cybersecurity if it cannot punish those who fail to comply.[82] A major part of the reporting requirement in the Act is that there are real consequences for those that fail to comply with the rules.[83] Currently, the Cybersecurity Framework is in place and run by the National Institute of Standards and Technology.[84] This program is voluntary, and companies seldomly release information about an attack on their systems because it makes a company look bad-hurting stock prices, public perception, and consumer confidence.[85] With no upside for reporting and large financial losses risked by reporting, companies have little incentive to do so.[86] Thus, private corporations in the critical infrastructure sectors must be required to report.

Failing to adhere may create a situation where valuable information capable of stopping the next big attack will go unlearned. The CIRO will not only require companies to report attacks, but it will have the power to bring enforcement actions for failure to report.[87] However, the consequences of the enforcement actions are very weak compared to the consequences of failing to report an attack.[88] All that the CISA can do when bringing an enforcement action is subpoena the

---

82. *See* Josephine Wolff, *Why It's So Hard to Punish Companies for Data Breaches*, THE N.Y. TIMES (Oct. 16, 2018), https://www.nytimes.com/2018/10/16/opinion/facebook-data-breach-regulation.html.

83. Andrew Serwin et al., *US Senate unanimously passes the Strengthening American Cybersecurity Act*, DLA PIPER (Mar. 14, 2022), https://www.dlapiper.com/en/us/insights/publications/2022/03/us-senate-unanimously-passes-the-strengthening-american-cybersecurity-act/.

84. *Cybersecurity Framework*, NAT'L INST. STANDARDS AND TECH., https://www.nist.gov/cyberframework (last visited Aug. 17, 2022).

85. *Id.*

86. *Id.*, *See* Danny Yadron, *Companies Wrestle with the Cost of Cybersecurity*, WALL ST. J. (Feb. 14, 2014), https://www.wsj.com/articles/SB10001424052702304834704579403421539734550.

87. Cyber Incident Reporting for Critical Infrastructure Act of 2021, H.R. 5440 § 2220A(g).

88. Brad Williams, *Mandatory Cyber Reporting Within 24 Hours: Sen. Warner Bill*, BREAKING DEF. (June 21, 2021, 5:12 PM), https://breakingdefense.com/2021/06/mandatory-cyber-incident-reporting-within-24-hours-sen-warner-bill/.

information that would have been required in the reporting, and if the entity does not comply, the CISA can bring a civil action.[89] Unfortunately, this will nullify the advantages of rapid disclosure by showing companies that there are no real consequences for failing to report an incident.

The CISA should be able to levy fines along with subpoenaing the requisite information. Allowing companies to prolong disclosure of attacks on systems with little but a slap on the wrist will hinder the agency's goal of remedying consequences of an attack and preventing similar attacks in the future. There needs to be serious monetary consequences if a company is going to put its own self-interest ahead of the safety of other critical infrastructure facilities and the country.

D. The Need For Periodic Disclosure

While the Cyber Incident Report Act makes great strides towards mandatory disclosures and creating preventative measures through data analysis in a centralized regulatory body, one improvement that it lacks is periodic reporting. The Act requires disclosure when an event occurs.[90] If an event does not occur, covered entities are not required to do anything else.[91]

An agency like the CISA should be able to have the CIRO require periodic filing with its office of the overall health of a company's data security systems. Such an exercise of authority could look similar to the SEC's mandatory, quarterly disclosure system.[92] There needs to be periodic reporting requirements like how the SEC requires quarterly reports that disclose a company's financial status, future prospects, and any material events affecting those.[93] The SEC requires these disclosures so that investors have all the information necessary to make informed investment decisions, markets remain as efficient as possible, and companies cannot commit fraud.[94]

Similarly, the CISA should require quarterly disclosures of a critical infrastructure firm's cyber security system. This could include disclosing the kinds of software being implemented, methods in place for catching attempted hacks, response plans if a hack is successful, and vulnerable infrastructure at the company's facilities. Creating such

---

89. Cyber Incident Reporting for Critical Infrastructure Act of 2021, §§ 2220A(g)(2)(A), (3)(A)-(B).

90. Cyber Incident Reporting for Critical Infrastructure Act of 2021, §§ 2220A(d)(1)(A), (d)(4), (d)(6).

91. *See id.*

92. William Johnson et al., *SEC Returns Spotlight to Cybersecurity Disclosure Enforcement,* HARV. L. SCH. F. ON CORP. GOVERNANCE (Aug. 1, 2021), https://corpgov.law.harvard.edu/2021/08/01/sec-returns-spotlight-to-cybersecurity-disclosure-enforcement/.

93. *Id.*

94. *Our Goals*, SEC, https://www.sec.gov/our-goals (last visited Jan. 23, 2022).

kinds of mandatory, periodic disclosures will give an agency like the CISA the ability to regulate who is doing a good job at protecting critical infrastructure facilities and who needs to take steps to increase its security.[95] This can create a much more preventative cybersecurity style than the proposed current reactionary regulations.[96] However, this will place vast amounts of extremely sensitive data in the hands of the CISA and make it a prime target for attacks. Proponents of small government intervention will argue this point, but private companies have done very little to show that the status quo provides sufficient protection.[97] Security standards for the CISA database will have to be higher than anywhere in the world, but it will be easier to control, monitor, and protect if all the data is based in a centralized location.

The SEC implements similar disclosure requirements so investors can tell how well a company is doing financially and how it might perform in the future.[98] Periodic disclosures for critical infrastructure firms would allow the CISA to see how strong cyber defenses are at places like nuclear power plants or pipeline facilities and how they will fare against cyberattacks in the future. With this information, the CISA can require that systems be updated to certain standards and fine those who fail to take proper steps to update and protect their cyber security systems. This will provide incentives for critical infrastructure firms to maintain strong cyber defenses as opposed to the current environment where firms would rather cut costs and have out-of-date systems.[99]

E. Security Concerns For Those Regulated

The overall goal of a regulatory body like the CISA should be to collect as much data as possible so it can formulate the best cyber defense strategies along with incentivizing critical infrastructure firms to take preventative action against hostile hacking. However, disclosure cannot be public like SEC disclosure due to the sensitive and compromising nature of the information to be collected by the CIRO.

---

95. The CISA will be able to access more sensitive information, not always disclosed to the public, when cyber incidents occur. An example of this type of occurrence is when the U.S. Cyber Command task force disclosed only some details to the public about a successful major cyber offensive operation against a significant cyber threat. Brett Tingley, *Cyber Command Task Force Conducted Its First Offensive Operation As The Secretary of Defense Watched*, THE WARZONE (Jan. 6, 2022), https://www.thedrive.com/the-war-zone/43776/cyber-command-task-force-conducted-its-first-offensive-operation-as-defense-secretary-watched.

96. *Reactive vs Proactive Cybersecurity*, TOUCHSTONE SEC., https://touchstonesecurity.com/reactive-vs-proactive-cybersecurity/#:~:text=A%20proactive%20cybersecurity%20strategy%20is,to%20prevent%20threats%20in%20advance (last visited Aug. 26, 2022).

97. *See, e.g.*, *New CFO Survey: More Than 80 Percent of Firms Say They've Been Hacked*, DUKE TODAY (Jun. 5, 2015), https://today.duke.edu/2015/06/cfohacking.

98. Johnson et. al., *supra* note 92.

99. *See* Catherine Sanders Reach, 2020 Budgeting & Planning, AM. BAR ASS'N: TECHREPORT 2020, (Dec. 7, 2020),https://www.americanbar.org/groups/law_practice/publications/techreport/2020/bp/.

Disclosure will need to be done in a confidential manner to ease worries about such compromising information being taken advantage of by hackers. The critical infrastructure private sector is responsible for the stability of everyday life in the United States, and they should be required to protect that stability to the best of their abilities. Financial motivations have provided little incentive for adopting stronger cyber defenses.[100]

While the Cyber Incident Reporting Act will be a step in the right direction if it passes, more structure and power need to be given to an agency like the CISA. Requiring periodic disclosure of the capabilities and vulnerabilities of cyber systems at these companies will make an agency like the CISA effective in delivering results that strengthen the cyber defenses of critical infrastructure companies and produce preventative measures against cyberattacks.

IV. CYBERSECURITY AND THE COURT SYSTEM

Currently, courts hold the company to a standard of reasonableness when a company is subject to a malicious hack that puts consumers at risk of some legally cognizable injury.[101] Companies can be found liable for data breaches if they do not implement reasonable security procedures to protect consumers.[102] Several legal experts have argued that there may exist a common law duty to provide adequate security for consumers of a company's product.[103] Of course, this creates a nightmare for courts staffed by judges with little experience in the field of cybersecurity who are trying to judge a company's actions with little case law to help guide their judgment.[104] This level of technical ambiguity creates inefficient court systems and lengthy cases.

A uniform set of regulations created by an agency like the CISA would make the court's job easier. Courts have found in the past that people can suffer legally cognizable injury from a data breach where their personal financial information was leaked.[105] Thus far, courts apply the reasonable and prudent business standard, which asks whether a reasonable and prudent business would have taken similar actions in a comparable situation, but this becomes foggy when multiple companies are involved in a data breach, with each pointing the finger

---

100. A. Etzioni, *The Private Sector: A Reluctant Partner in Cybersecurity*, GEO. WASH. UNIV. INST. FOR COMMUNITARIAN POL'Y STUD. (Dec. 19, 2014), https://icps.gwu.edu/private-sector-reluctant-partner-cybersecurity.

101. In re Equifax Inc. Sec. Litig., 362 F. Supp. 3d 1295, 1323 (N.D. Ga. 2019).

102. Thomas J. Smedinghoff, *The Developing U.S. Legal Standard for Cybersecurity*, 4 SEDONA CONF. J. 109, 109 (2003).

103. *Id.* at 111.

104. *See id.*

105. *See In re Equifax,* 362 F. Supp. 3d at 1317.

at the other.[106] Federal standards and required disclosures of cybersecurity systems could alleviate the initial burden on courts to sift through complex cybersecurity matters when determining liability if there were a federal agency that was already monitoring the situation closely.

In 2017, Equifax's customer database was infiltrated by hackers who stole customer names, Social Security numbers, birthdates, and addresses, affecting more than half of the U.S. population.[107] Investors brought a securities suit alleging that Equifax misled investors about its cybersecurity capabilities.[108] The court found that Equifax misled investors by stating that its cybersecurity was up to industry standards while, in reality, there were widespread deficiencies in their cyber defense systems.[109] Equifax's internal security system was so bad that the court determined Equifax's efforts "demonstrated a systemic disregard for cybersecurity"[110] and failed to meet the most basic industry standards.[111] The court discussed the reasonableness standard as one based on customs in that industry.[112]

Unfortunately, federal judges are often older and have little technology experience.[113] Lack of expertise in specific and technical fields is a problem often faced in the American legal system when judges are forced to pass judgment on matters that are hard to understand without years of experience in the given field.[114] The same can be true for juries as well.[115] Luckily for the court in *Equifax*, the conduct was so against what a reasonable company in Equifax's shoes would do that one did not need a degree in computer science to understand something was wrong.[116] However, when a situation occurs like that in the SolarWinds story, matters become much more technical and industry-related to the point where one would need to understand how these cybersecurity systems operate to pass fair judgment on the actions of companies.

---

106. Stark, *supra* note 16.

107. Alfred Ng, *How the Equifax hack happened, and what still needs to be done*, CNET (Sept. 7, 2018), https://www.cnet.com/tech/services-and-software/equifaxs-hack-one-year-later-a-look-back-at-how-it-happened-and-whats-*changed/*.

108. *In re Equifax Inc. Sec. Litig*., 357 F.Supp.3d 1189, 1205, 1214 (N.D. Ga. 2019).

109. *Id*. at 1219–20, 1228.

110. *Id*. at 1228.

111. *See id*. at 1219-20 (affirming allegations that Equifax's cybersecurity systems were below industry standards).

112. *Id*.

113. David O. Taylor, *Formalism and Antiformalism in Patent Law Adjudication: Rules and Standards*, 46 CONN. L. REV. 415, 494 (2013) (discussing Justice Scalia's concession that even he has little expertise in patent law and how federal judges' lack of expertise in complex patent issues creates bad law).

114. *See, e.g., id.* at 483.

115. *Id*. at 482-83.

116. *In re Equifax Inc. Sec. Litig.*, 357 F. Supp. 3d 1189, 1229 (N.D. Ga. 2019).

To ensure efficient and fair judgment against companies that fail to protect critical infrastructure systems, a separate court system like the tax courts could alleviate the disparity between complex cyberattacks and judges who know little about how cybersecurity systems operate. Under the Constitution, Congress has the power to create such court systems.[117] Judges could become experts in understanding the right and wrong ways of protecting critical infrastructure systems.[118] The reasonableness standard will become more clearly defined not just by the proposed regulations but also by judges who will be experts in cybersecurity. Such a court system would also allow disputes to be confidential so an evaluation of all information and the entire story of what happened can take place.[119]

Moreover, as technology expands, more and more companies will have to integrate with the cyber world, meaning there will likely be an uptick in litigation regarding cybersecurity incidents as cyberattacks increase.[120] Companies will be more willing to beef up their cybersecurity systems if they know there is a real chance of punishment by a court that thoroughly understands how cybersecurity systems should work and how companies try to cut corners to save money. Not only will such a court system make sure companies are held accountable, but these courts will be able to handle the caseload in a much more efficient and timely manner.[121] Time is critical in cybersecurity, and having a court system that can handle cases consistently and efficiently will allow the truth about a hack to be known so appropriate responses can be taken and companies can be held accountable before the attack. This new court system needs to be quick and exclusive to cybersecurity cases because it could mean the difference between stopping the next hack on a nuclear powerplant or the entire grid going down on the East Coast.

Creating a clear standard of reasonableness begins with new regulations that can chart a path for what companies need to be doing

---

117. U.S. CONST. art. I, § 8, cl. 9.

118. *See* Roger A. Grimes, *Why it's so hard to Prosecute Cyber Criminals*, CSO (Dec. 6, 2016), https://www.csoonline.com/article/3147398/why-its-so-hard-to-prosecute-cyber-criminals.html.

119. *See* Laura L. Donohue, *The Shadow of State Secrets*, 159 U. PA. L. REV. 77, 95-97 (2010) (discussing the use of the state secrets privilege by corporations owning critical information infrastructure to keep information critical to national security from being released to the public through court proceedings).

120. *See* Caitlin McFall, *As Cyberattack Threats Rise, Expert Reveals 'nightmare scenario'*, FOXBUSINESS (Jan. 28, 2022, 5:31 PM), https://www.foxbusiness.com/politics/cyberattack-threats-expert-reveals-nightmare-scenario (explaining that the American infrastructure system is going through a digital transformation which creates a much more significant ability for malicious hackers to attack the U.S. industrial infrastructure).

121. *Cf.* Henry Y. Huang, *A new "rocket docket" for Patent Litigation in the US*, WHITE & CASE LLP (Sept. 18, 2020), https://www.whitecase.com/insight-our-thinking/new-rocket-docket-patent-litigation-us (describing Judge Alan Albright's "rocket docket" as rapid and friendly to patent plaintiffs).

to prevent cyberattacks. Developing case law in specialized cyber courts will create efficient responses to attacks and layout what actions constitute reasonable responses. Clear standards based on expert judgments from specialized courts will show companies what needs to be done to prevent cyberattacks without fear of fines or litigation.

V. CONCLUSION

The current state of laws regulating the cybersecurity of critical infrastructure is void of any meaningful impact on how private companies in critical infrastructure sectors of the American economy go about protecting infrastructure systems that keep the country alive and running. The companies have shown that monetary incentives will almost certainly outweigh any consideration given to the societal benefit of spending a little more money for stronger cyber defense systems.

The United States must adopt a clear set of regulations that incentivize private companies to take a more preventive, rather than reactionary, approach to protect critical infrastructure systems from cyberattacks. Creating a regulatory body that mandates regular confidential disclosure of the health of a company's cybersecurity capabilities along with allowing that agency to punish those who fail to meet the standards set by the agency will provide the country with a much-needed upgrade for the nation's cyber defense of critical infrastructure. Furthermore, the agency will be able to monitor the safety of systems such as nuclear power plants and water treatment facilities in the event of an attack by a malevolent hacker.

Moreover, a separate court system like the tax courts should be created to ensure that complex cybersecurity incidents are handled fairly, efficiently, and in a manner that sets a well thought out standard of reasonableness.

The inability of profit-driven private companies to adequately protect U.S. critical infrastructure will lead to devastating consequences if regulations are not put in place to change how companies use cybersecurity systems to protect critical infrastructure systems from cyberattacks.