Indiana Law Review

Volume 55 **2022** **Number 4**

ARTICLES

(RE-)CONFIGURING FEDERAL CYBERSECURITY REGULATION: FROM CRITICAL INFRASTRUCTURES TO THE WHOLE-OF-THE-NATION

GRAHAM STREICH*

ABSTRACT

Cyberattacks are one of the greatest threats to the United States' national security. Facing an increase in cyberattacks, the current patchwork of federal cybersecurity regulations does not maximize the country's ex ante defense that should protect the entire nation. This Article examines federal agencies' involvement in promulgating cybersecurity regulations and Executive Branch cybersecurity actions, identifying three shortcomings in the current framework: (1) the nation lacks a general cybersecurity agency with regulatory and enforcement authority, (2) cybersecurity programs often rely on business participation and leadership without incorporating non-profit organizations and individuals, and (3) cybersecurity approaches often overemphasize the importance of attributing attacks to the corresponding culprits. To rectify these weaknesses and maximize cyber defense, this Article argues that Congress should expand the Cybersecurity and Infrastructure Security Agency's rulemaking and enforcement authority to monitor and mitigate cyber threats across varying sectors, including government, businesses, insurers, non-profit organizations, and individuals.

* J.D. Candidate, 2023, Fordham University School of Law; B.S. & B.A., 2019, New York University. I want to thank Professors Thomas Lee and Olivier Sylvain for their support throughout the drafting process. The views expressed, along with any omissions or errors, remain the Author's own.

TABLE OF CONTENTS

INTRODUCTION

Cyberattacks are considered the greatest threat to the United States' national security[1] and are central to competition among the great global powers;[2] however,

1. *See* Jim Garamone, *Cyber Tops List of Threats to U.S., Director of National Intelligence Says*, DEP'T DEF. NEWS (Feb. 13, 2018), https://www.defense.gov/News/News-Stories/Article/Article/1440838/cyber-tops-list-of-threats-to-us-director-of-national-intelligence-says/ [perma.cc/6DKW-JTLJ]; Dustin Volz & David Uberti, *Biden Says Cybersecurity Is the 'Core National Security Challenge' at CEO Summit*, WALL ST. J. (Aug. 25, 2021), https://www.wsj.com/articles/biden-to-hold-cybersecurity-summit-with-tech-giants-top-banks-energy-firms-11629882002 [perma.cc/65KF-853D].

2. *See* Robert D. Williams, *Reckoning with Cyberpolicy Contradictions in Great Power Politics*, BROOKINGS INST. (Oct. 12, 2021), https://www.brookings.edu/techstream/reckoning-with-

current contradictory patchwork federal cybersecurity policies do not maximize the nation's cyber defense.[3] Between December 2020 and May 2021, the United States suffered two of the worst cyberattacks in the country's history.[4]

In December 2020, FireEye, a cybersecurity company, reported the SolarWinds Hack, a cyberattack that used a routine SolarWinds software update to inject malicious code into users' computers.[5] The SolarWinds Hack was one of the worst espionage attacks in the history of the United States because of the size and importance of the victims, including the Cybersecurity and Infrastructure Security Agency (CISA or "the Agency")—the Agency within the Department of Homeland Security (DHS or "the Department") mandated to defend federal computer networks.[6] While the total harm from the SolarWinds Hack is challenging to measure, some estimates indicate a potential eighteen-month recovery period and costs around one hundred billion dollars.[7]

In May 2021, Colonial Pipeline, the United States' largest pipeline for refined oil, was attacked with ransomware through a standard virtual private network account with single-factor authentication, causing panic up and down the East Coast.[8] Thousands of people hoarded gasoline in response, causing dire fuel

---

cyberpolicy-contradictions-in-great-power-politics/ [perma.cc/P8U8-3AF8].

3. *See* Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN REL. (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection [perma.cc/APT5-8HL5]; Terry Thompson, *The Colonial Pipeline Cyber Attack and the SolarWinds Hack Were All but Inevitable. Why National Cyber Defense Is a 'Wicked' Problem*, VA. MERCURY (May 13, 2021), https://www.virginiamercury.com/2021/05/13/the-colonial-pipeline-cyber-attack-and-the-solarwinds-hack-were-all-but-inevitable-why-national-cyber-defense-is-a-wicked-problem/ [perma.cc/LC75-TZEV]; *infra* notes 168-217 and accompanying text.

4. *See* Thompson, *supra* note 3.

5. *See* Dina Temple-Raston, *A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Hack*, NPR (Apr. 16, 2021), https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack [perma.cc/FA56-5AET].

6. *See* 6 U.S.C. § 652 (2018) (giving CISA wide authority within federal government); Temple-Raston, *supra* note 5.

7. *See* Patrick Howell O'Neill, *Recovering from the SolarWinds Hack Could Take 18 Months*, MIT TECH. REV. (Mar. 2, 2021), https://www.technologyreview.com/2021/03/02/1020166/solarwinds-brandon-wales-hack-recovery-18-months/ [perma.cc/P5R8-ZR2L]; Gopal Ratnam, *Cleaning Up SolarWinds Hack May Cost as Much as $100 Billion*, ROLL CALL (Jan. 11, 2021), https://www.rollcall.com/2021/01/11/cleaning-up-solarwinds-hack-may-cost-as-much-as-100-billion/ [perma.cc/9R9H-BHCJ].

8. *See* 167 CONG. REC. H2,547 (daily ed. May 19, 2021) (statement of Rep. Jim Himes); 167 CONG. REC. H2,299 (daily ed. May 13, 2021) (statement of Rep. Doug LaMalfa); 167 CONG. REC. S4, 024 (daily ed. June 10, 2021) (statement of Sen. Chuck Schumer); *Threats to Critical Infrastructure: Examining the Colonial Pipeline Cyber Attack: Hearing on SD-342 Before S. Comm. on Homeland Security & Gov't Affairs*, 117th Cong. (June 8, 2021) (statement of Joseph A. Blount, JR., President and Chief Executive Officer, Colonial Pipeline).

shortages.[9] The attack forced Colonial Pipeline to stop its principal operations until it paid the hackers' ransom of seventy-five Bitcoins with the Federal Bureau of Investigation's (FBI) assistance, an amount then valued at $4,400,000.[10] Although the Department of Justice (DOJ) reported recovering nearly sixty-four of the Bitcoins, the value of Bitcoin dropped, resulting in an estimated recovery of only $2,300,000.[11] Other, potentially more harmful consequences, such as the resulting increase in gasoline prices, cost to taxpayers for the FBI's involvement, and general fear, were not restituted.[12]

National cyberattacks, like SolarWinds and Colonial Pipeline, received attention and quick responses[13] and perhaps even motivated the Biden Administration's later cybersecurity policy.[14] But, more significant attacks obscure the reality that most cyberattacks target smaller businesses, organizations,

---

9. *See* Vanessa Romo, *Panic Drives Gas Shortages After Colonial Pipeline Ransomware Attack*, NPR (May 11, 2021, 10:21 PM), https://www.npr.org/2021/05/11/996044288/panic-drives-gas-shortages-after-colonial-pipeline-ransomware-attack [perma.cc/VQ4P-KJH3].

10. *See* Collin Eaton & Dustin Volz, *Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom*, WALL ST. J. (May 19, 2021), https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636 [perma.cc/G6HD-7DT2].

11. *See* Press Release 21-528, Dep't of Just., Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside (June 7, 2021), https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside [perma.cc/BDF2-7C6X].

12. *See* Catherine Thorbecke, *Gas Hits Highest Price in 6 Years, Fuel Outages Persist Despite Colonial Pipeline Restart*, ABC NEWS (May 27, 2021), https://abcnews.go.com/US/gas-hits-highest-price-years-fuel-outages-persist/story?id=77735010 [perma.cc/A63B-UP3Q].

13. *See* Press Conference, The White House, Remarks by President Biden on the Colonial Pipeline Incident, (May 13, 2021), https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/05/13/remarks-by-president-biden-on-the-colonial-pipeline-incident/ [perma.cc/YYU4-DDFG]; Press Release, The White House, Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government (Apr. 15, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/ [perma.cc/C4J8-2XN2]; Natasha Bertrand et al., *Colonial Pipeline Did Pay Ransom to Hackers, Sources Now Say*, CNN (May 13, 2021, 7:00 PM), https://www.cnn.com/2021/05/12/politics/colonial-pipeline-ransomware-payment/index.html [perma.cc/HSL7-PM7E]; Collin Eaton & Amrith Ramkumar, *Colonial Pipeline Shutdown: Is There a Gas Shortage and When Will the Pipeline Be Fixed?*, WALL ST. J. (May 13, 2021, 11:07 AM) https://www.wsj.com/articles/colonial-pipeline-cyberattack-hack-11620668583 [perma.cc/B8MT-7TL2]; Lucas Ropek, *SolarWinds Scandal Calls Attention to Supply Chain Security*, GOV. TECH. (Dec. 17, 2020), https://www.govtech.com/security/solarwinds-scandal-calls-attention-to-supply-chain-security.html [perma.cc/52EG-T7PF]; David E. Sanger et al., *Major Pipeline Forced to Close By Cyberattack*, N.Y. TIMES (May 9, 2021), at A1.

14. *See* David P. Fidler, *America's Place in Cyberspace: The Biden Administration's Cyber Strategy Takes Shape*, COUNCIL ON FOREIGN REL. (Mar. 11, 2021), https://www.cfr.org/blog/americas-place-cyberspace-biden-administrations-cyber-strategy-takes-shape [perma.cc/4GMK-BFLX].

and individuals who do not receive the same response or attention as larger attacks.[15]

Cyberattacks will increase in frequency and sophistication, wreaking greater havoc across all industries and people in the United States.[16] The United States' contradictory patchwork cybersecurity approach leaves the nation's infrastructure unprepared for attacks and does not maximize threat defense or deterrence.[17] Despite grave cybersecurity threats, current piecemeal state and federal cybersecurity, and consumer privacy legislation, are lacking.[18] Current

---

15. *See* Statement, Sec. Exch. Comm'n, Commissioner Luis A. Aguilar, The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses (Oct. 19, 2015), https://www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize-businesses.html [perma.cc/UF2S-2494]; Kellen Browning, *Ransomware Salvo Hits Eight Hundred to One Thousand and Five Hundred Businesse*s, N.Y. TIMES (July 6, 2021), at B4; Robert McMillian et al., *Beyond Colonial Pipeline, Ransomware Cyberattacks Are a Growing Threat*, WALL ST. J. (May 11, 2021), https://www.wsj.com/articles/colonial-pipeline-hack-shows-ransomware-emergence-as-industrial-scale-threat-11620749675 [perma.cc/WE6M-QCF6]; Eric Rosenbaum, *Main Street Over Confidence: America's Small Businesses Are Not Worried About Hacking*, CNBC (Aug. 10, 2021), https://www.cnbc.com/2021/08/10/main-street-overconfidence-small-businesses-don't-worry-about-hacking.html [perma.cc/G4YK-K2Fb].

16. *See* Max Fisher, *Constant but Camouflaged, Flurry of Cyberattacks Offers Glimpse of New Era*, N.Y. TIMES (July 20, 2021), https://www.nytimes.com/2021/07/20/world/global-cyberattacks.html [perma.cc/5RLZ-D9DD] (describing widespread government-linked hacking and why these hacks are here to stay); Lynsey Jeffery & Vignesh Ramachandran, *Why Ransomware Attacks Are on The Rise—And What Can Be Done to Stop Them*, PBS (July 8, 2021, 3:28 PM), https://www.pbs.org/newshour/nation/why-ransomware-attacks-are-on-the-rise-and-what-can-be-done-to-stop-them [perma.cc/VG27-LU97] (discussing how ransomware attacks are increasing in both frequency and profile); Samara Lynn & Catherine Thorbecke, *Why Ransomware Cyberattacks Are On the Rise*, ABC NEWS (June 4, 2021), https://abcnews.go.com/Technology/ransomware-cyberattacks-rise/story?id=77832650 [perma.cc/HL3E-FVYD] (explaining increased ransomware attacks as a confluence of factors including hard-to-trace cryptocurrency, more opportunities because of more working from home, and increasing political tension, specifically between the United States and Russia).

17. *See generally* U.S. GOV'T ACCOUNTABILITY OFF., GAO-19-128, WEAPONS SYSTEM CYBERSECURITY (2018), https://www.gao.gov/assets/gao-19-128.pdf [perma.cc/UW3A-G5XG] (describing the extent of United States cybersecurity vulnerabilities); ROB PORTMAN & CARY PETERS, STAFF OF S. COMM. ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS, FEDERAL CYBERSECURITY: AMERICA'S DATA *STILL* AT RISK (2021), https://www.hsgac.senate.gov/imo/media/doc/Federal%20Cybersecurity%20-%20America's%20Data%20Still%20at%20Risk%20(FINAL).pdf [perma.cc/9WVW-9VNH] (discussing remaining cyber vulnerabilities in federal government post-CISA); Jeff Kosseff, *Hacking Cybersecurity Law*, 2020 U. ILL. L. REV. 811, 818-19 (2020) (arguing that the primary systemic problem in United States cybersecurity is the misunderstanding of how components function as a whole).

18. *See* Press Release, The White House, Fact Sheet: Biden Administration Announces Further Actions to Protect U.S. Critical Infrastructure (July 28, 2021), https://www.whitehouse.gov/briefing-

cybersecurity regulation is entity or industry-specific, with the Federal Trade Commission (FTC) and Securities Exchange Commission (SEC) as enforcers of private sector cybersecurity.[19] The Executive's national security powers also regulate cybersecurity.[20] Though President Joseph Biden embraced a "whole-of-[the]-nation" approach to cybersecurity, his Executive Orders focused on critical infrastructures and private sector cooperation.[21] Consequently, these laws and Executive Orders do not ensure robust cyber defense protocols across the nation and centralized cyber threat monitoring[22] or maximize transparency and certainty for citizens, companies, and insurers.[23]

Instead, current legislation dichotomizes data protection and privacy from cyberattacks,[24] relies on decentralized reporting and self-regulation,[25] and focuses on attributing the attack to a specific entity.[26] These weaknesses may complicate

---

room/statements-releases/2021/07/28/fact-sheet-biden-administration-announces-further-actions-to-protect-u-s-critical-infrastructure/ [perma.cc/MJ85-FPWB] (describing federal cybersecurity as a piecemeal patchwork of sector-specific statutes that, given the evolving cyber threats the nation faces, recommends new voluntary and mandatory approaches).

19. *See infra* notes 42-55 and accompanying text.

20. *See generally* David W. Opderbeck, *Cybersecurity and Executive Power*, 89 WASH. UNIV. L. REV. 795, 812-26 (2012) (describing the Executive Branch's power over cybersecurity).

21. *See infra* Section I.C.

22. *See, e.g.*, PORTMAN & PETERS, *supra* note 17 (warning that the federal government is not preprepared for the dynamic cyber threats that exist today); Timothy Gardner, *Analysis: Cyberattack Exposes Lack of Required Defenses on U.S. Pipelines*, REUTERS (May 12, 2021), https://www.reuters.com/technology/cyberattack-exposes-lack-required-defenses-us-pipelines-2021-05-12/ (explaining the lack of mandatory cybersecurity procedures for pipelines compared to electrical grids).

23. *See generally* William H. Dutton et al., *Cybersecurity Capacity: Does it Matter?*, 9 J. INFO. POL'Y 280, 288 (2019) (explaining that lack of trust and transparency hinder cybersecurity); Eldar Haber & Tal Zarsky, *Cybersecurity for Infrastructure: A Critical Analysis*, 33 FLA. ST. UNIV. L. REV. 515, 571 (2016) (arguing that cybersecurity transparency mitigates potential rights violations and reduces fear).

24. *See* Jeff Kosseff, *Congress Is Finally Tackling Privacy! Now Let's Do Cybersecurity*, SLATE (Dec. 3, 2019), https://slate.com/technology/2019/12/congress-national-privacy-law-cybersecurity.html [perma.cc/4HAM-KHCK] (explaining how cybersecurity and data privacy are distinct but interrelated and that government must devote equal attention to each issue).

25. *See Cybersecurity: Assessing the Immediate Threat to the United States: Hearing Before the Subcomm. On Nat'l Sec. Homeland Def. and Foreign Operations*, 112th Cong. 24-32 (2011) (statement of James A. Lewis, Director, Ctr. For Strategic and Int'l Stud.) (stating that self-regulation is inadequate for national security, specifically cybersecurity, because the most important function for companies is to make money not develop defense).

26. *See generally* Florian J. Egloff & Max Smeets, *Publicly Attributing Cyber Attacks: A Framework*, J. STRATEGIC STUD. 1, 3, 21-22 (2021), https://www.tandfonline.com/doi/pdf/10.1080/01402390.2021.1895117?needAccess=true [perma.cc/K5MJ-W4UD] (arguing that an attribution framework should be strategic, coordinated, and pragmatic with flexibility to determine the appropriateness of attribution on a case-by-case basis); Martha Finnemore, *Beyond Naming and*

investigations and, if the suspected culprit is a foreign actor, they will unlikely be extradited to the United States, making complicated investigations unfruitful.[27] While security systems cannot be perfectly secure, Congress can significantly improve cybersecurity and defense.[28]

Though Congress created the CISA to develop guidance for sharing cyber threat indicators, the Agency lacks regulatory or enforcement power outside the federal government.[29] The 9/11 terrorist attacks in the United States demonstrated how essential centralizing information is for security,[30] yet CISA cannot mandate non-federal government entities to share cyber threat indicators.[31] Current cybersecurity regulations leave the United States' cyber infrastructure underprepared for inevitable attacks.[32]

Post-9/11 government actions also show democratic pitfalls in national security policy stemming from the supposed tradeoff between security and liberty.[33] For instance, in 2002, the National Security Agency (NSA) began eavesdropping domestically without warrants to search for terrorist activity.[34] This revelation instigated an audit of the NSA; nonetheless, the NSA's domestic surveillance program expanded in 2007 with the PRISM program, which included back doors for the NSA to gather information from multiple big technology companies.[35]

Shaming: Accusations and International Law in Cybersecurity, 31 EUR. J. INT. L. 969, 970 (2020) (explaining that attribution stymies international rules regarding cyber operations that target civilians outside of armed conflicts); Chris O'Brien, *Why is 'Attribution' Still the Focus Following Cyber Attacks?*, INFO. SEC. MAG., (Nov. 23, 2018), https://www.infosecurity-magazine.com/opinions/attribution-focus-attacks/ [perma.cc/4N5X-2FNB] (questioning the utility of attribution in cybersecurity).

27. *See generally* Finnemore, *supra* note 26 (discussing the attribution problem in cybersecurity given multiple jurisdictions and extradition agreements).

28. *See* Shuman Ghosemajumder, *You Can't Secure 100% of Your Data 100% of the Time*, HARV. BUS. REV. (Dec. 4, 2017), https://hbr.org/2017/12/you-cant-secure-100-of-your-data-100-of-the-time [perma.cc/7JM4-5XPL] (describing the impossibility of perfect cybersecurity).

29. *See infra* notes 102-10 and accompanying text.

30. *See infra* notes 167-80 and accompanying text.

31. *See infra* notes 102-10 and accompanying text.

32. *See infra* notes 168-89 and accompanying text.

33. *See generally* Tiberiu Dragu, *Is There a Trade-off Between Security and Liberty? Executive Bias, Privacy Protections, and Terrorism Prevention*, 105 AM. POL. SCI. REV. 64, 812-26 (2011) (describing and empirically questioning the supposed trad-off between national security and liberty); Julian Sanchez, *Talking About "Trade offs" Between Liberty and Security Begs the Question*, CATO BLOG (July 26, 2012), https://www.cato.org/blog/talking-about-trade-offs-between-liberty-security-begs-question [perma.cc/562G-6XMW] (questioning whether security improved given the increased post-9/11 government surveillance that come at liberty's expense).

34. *See* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES (Dec. 16, 2005), at A1.

35. *See* Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of*

Cybersecurity agencies need accountability given the power for abuse that can accompany security legislation.[36] As this Article argues, CISA needs cybersecurity rulemaking authority and enforcement power across the United States.[37] Expanding CISA's authority would improve the defense and resiliency of the United States' overall cybersecurity while enhancing democratic values like transparency and pluralism.[38]

Section I.A begins with a discussion of the current federal cybersecurity regulatory regime. Section I.B then discusses the DOJ's dual role of enforcing other federal agencies' cyber regulation and prosecuting cybercrimes. Section II.C explains the Biden Administration's cybersecurity Executive Orders, memos, and overall approach to cybersecurity. Section I.D introduces congressionally proposed cybersecurity policies. And Section I.E presents other suggested cybersecurity improvements, including (1) sanctioning ransomware payments, (2) creating a federal cyber insurance policy, and (3) treating cyber infrastructure as an abnormally dangerous activity with strict liability.

Part II discusses three primary insufficiencies of current and proposed cybersecurity regulations. This Part begins by explaining how patchwork security framework diminishes ex ante defense with pre-and-post-9/11 national security legislation. Part II also identifies three primary weaknesses in current and proposed federal cybersecurity regulation.

Section III.A argues that expanding CISA's rulemaking and enforcement authority would mitigate current federal cybersecurity shortcomings identified in Part II. Section III.B discusses how providing CISA with these regulatory tools would enhance ex ante cyber defense across the United States, without supplanting existing regulation, by centralizing general cybersecurity authority. Section III.C discusses how rulemaking allows all types of parties, not just businesses, access to cybersecurity defense. Additionally, Section III.D argues that fostering robust cyber defense through regulation would prevent cyberattacks by providing ex ante cybersecurity in the first place and thus avoid attributing cyberattacks to their culprits.

I. CURRENT APPROACHES TO CYBER AND DATA SECURITY

The United States Congress has not created a general statute requiring data and cybersecurity protocols across all industries and sectors.[39] Instead, except for designated "critical" industries, companies are incentivized, but not required, to

---

Apple, Google and Others, THE GUARDIAN (June 7, 2013), https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data [perma.cc/PY9D-32GR].

36. *See* Carrie Cordero, *Reforming the Department of Homeland Security Through Enhanced Oversight & Accountability*, CTR. FOR NEW AM. SECURITY (May 12, 2020), https://www.cnas.org/publications/reports/reforming-the-department-of-homeland-security-through-enhanced-oversight-accountability [perma.cc/X5RH-2DPT].

37. *See infra* Part III.

38. *See id.*

39. *See* Kosseff, *supra* note 17, at 811, 815.

share cybersecurity threat indicators and defensive measures with the federal government and other entities such as cyber insurers.[40]

Section I.A of this Article summarizes the different federal agencies that create the nation's patchwork cybersecurity framework. Section I.B discusses the DOJ's role in enforcing cyber regulations and laws and extradition problems that frequently occur with cybercrimes. Section I.C explains President Biden's approach to cybersecurity, and Section I.D introduces a congressionally proposed cybersecurity act that would apply generally. Section I.E discusses three other proposed improvements for national cybersecurity.

A. Federal Cybersecurity Patchwork Regulation

Federal cybersecurity regulation relies on sector or function-specific agencies, not centralized authority.[41] Section I.A.1 introduces the SEC's financial institution cyber regulation. Section I.A.2 discusses the FTC's authority and circuit court's deference to FTC enforcement orders. Section I.A.3 explains how the United States Department of the Treasury (Treasury) combats rising ransomware cyberattacks by sanctioning cryptocurrency payments from certain nations. Section I.A.4 discusses the National Institute of Standards and Technology's (NIST or "the Institute") expertise in providing technical guidance to regulatory agencies. Section I.A.5 introduces the DHS' national security power and role in regulating critical industries. Section I.A.6 discusses how Congress created CISA and the Agency's limited regulatory authority.

1. Securities and Exchange Commission.—Congress gave the SEC explicit authority over data security through the Gramm-Leach-Bliley Act of 1999,[42] which requires financial institutions to disclose their information-sharing practices and safeguard sensitive data.[43] In 2017, the SEC expanded their cybersecurity regulation and enforcement by creating a cyber unit that focuses "on targeting cyber-related misconduct and the establishment of a retail strategy task force that will implement initiatives that directly affect retail investors . . . ."[44] In 2018, the SEC released interpretive guidance that clarified public companies' duties to disclose material cybersecurity risks and incidents to investors.[45] Since creating this unit and guidance, the SEC has investigated and brought enforcement actions against regulated companies that do not comply with

---

40. *See id*. at 815-19.

41. *See id*. at 815-16.

42. 15 U.S.C. §§ 6801-6809 (1999).

43. 15 U.S.C. § 6801 (1999).

44. Press Release, Sec. Exch. Comm'n, SEC Announces Enforcement Initiatives to Combat Cyber-Based Threats and Protect Retail Investors (Sept. 25, 2017), https://www.sec.gov/news/press-release/2017-176 [perma.cc/BJQ7-SBYQ].

45. *See* 17 C.F.R. §§ 229, 249 (2018); Rebecca Rabinowitz, *From Securities to Cybersecurity: The SEC Zeroes in on Cybersecurity*, 61 B.C. L. REV. 1535, 1538-39 (2020).

data safeguards or report data breaches deficiently.[46]

The SEC can bring civil liability suits against regulated companies but may only issue criminal charges through the DOJ utilizing mutual legal assistance treaties (MLATs).[47] This arrangement focuses on realized injuries and ex post enforcement, not ex ante defense.[48] For instance, on January 15, 2021, the SEC began investigating SolarWinds under CISA's directions.[49] The SEC requested certain parties voluntarily share whether they downloaded a compromised version of SolarWinds software, among other information.[50] But, Congress limited the SEC's mandate to designated industries, including public companies and companies significantly engaged in providing financial products or services.[51]

2. Federal Trade Commission.—The FTC has interpreted § 5 of the Federal Trade Commission Act[52] regarding unfair or deceptive acts in commerce as providing some data and privacy regulatory authority based on companies' deficient cybersecurity protocols which fail to protect consumer data against hackers.[53] Consequently, the FTC brought dozens of enforcement actions against companies that allegedly lied about data security practices or failed to safeguard information.[54] Although the FTC is the closest thing to a general cybersecurity

---

46. *See Threats to Critical Infrastructure: Examining the Colonial Pipeline Cyber Attack: Hearing on SD-342 Before S. Comm. on Homeland Sec. & Gov't Affairs*, 117th Cong. (2021) (statement of Joseph A. Blount, JR., President and Chief Executive Officer, Colonial Pipeline).

47. *See* U.S. SECURITIES AND EXCHANGE COMMISSION, ENFORCEMENT MANUEL (2017), https://www.sec.gov/divisions/enforce/enforcementmanual.pdf [perma.cc/E9LH-K2WD].

48. *See* Samuel Issacharoff, *Regulating After the Fact*, 56 DEPAUL L. REV. 375, 379-80 (2007) (explaining the SEC's ex post enforcement model is premised on the idea that parties should internalize the risk of liability and self-regulate accordingly).

49. *See* U.S. SEC. & EXCHANGE COMMISSION, FINAL MANAGEMENT LETTER: REVIEW OF THE SEC'S COMPLIANCE WITH CISA EMERGENCY DIRECTIVE 21-01 AND INITIAL RESPONSE TO THE SOLARWINDS COMPROMISE (2021), https://www.sec.gov/files/Final-Management-Letter-Review-of-the-SEC-Compliance-with-CISA-ED-21-01-and-Initial-Response-to-the-SolarWinds-Compromise.pdf [perma.cc/L4CW-EARZ].

50. *See In the Matter of Certain Cybersecurity—Related Events (HO-14225) FAQs*, U.S. SEC. & EXCHANGE COMMISSION (June 25, 2021), https://www.sec.gov/enforce/certain-cybersecurity-related-events-faqs [https://perma.cc/D6DA-4V6W]; Christopher Bing et. al., *Wide-Ranging SolarWinds Probe Sparks Fear in Corporate America*, REUTERS (Sept. 10, 2021), https://www.reuters.com/technology/exclusive-wide-ranging-solarwinds-probe-sparks-fear-corporate-america-2021-09-10/ [https://perma.cc/3E79-ARC3].

51. *See* 16 C.F.R. § 314 (2016). *See generally* Nick Oberheiden, *Gramm Leach Bliley Act: Two Requirements & Seven Ways to Achieve Compliance*, 9 NAT'L L. REV. 154 (2021) (describing how the SEC regulates financial institutions).

52. 15 U.S.C. §§ 41-58 (1914).

53. *See* GINA STEVENS, CONG. RES. SERV., R43723, THE FEDERAL TRADE COMMISSION'S REGULATION OF DATA SECURITY UNDER ITS UNFAIR OR DECEPTIVE ACTS OR PRACTICES (UDAP) AUTHORITY 1-2 (2014), https://sgp.fas.org/crs/misc/R43723.pdf [perma.cc/KEH7-PS88].

54. *See, e.g.*, DSW Inc., 52 F.T.C. 3096 (2006); Superior Mortgage Corp., 52 F.T.C. 3136 (2005); BJ's Wholesale Club, Inc. 42 F.T.C. 3160 (2005); Vision I Properties, LLC, et. al., 42 F.T.C.

regulator that the United States has,[55] the Third and Eleventh Circuits disagree over the scope of the FTC's authority.[56]

Two main hurdles to the FTC's enforcement are the pre-internet context of the FTC's mandate[57] and the FTC's limited rulemaking authority.[58] In *FTC v. Wyndham Worldwide Corp.*,[59] after the defendant suffered three cyber hacks, the FTC brought an enforcement order against the defendant company.[60] The FTC's enforcement order found that the defendant did *not* use readily available security measures, specifically firewalls, encryption, other commercially reasonable methods of protecting consumer data, or follow the appropriate incident response procedures in the FTC's nonbinding guidebook on safeguarding personal information.[61] The defendant argued that the FTC's relevant rules regarding cybersecurity were too vague to give the company notice of required cybersecurity measures and, thus, the FTC abused its discretion by using adjudication against Wyndham without first giving Wyndham notice of the regulation through rulemaking or other binding agency action.[62] The Third Circuit found the defendant's argument unconvincing because it should have been "painfully clear" to the defendant that it failed the statutorily required cost-benefit analysis after the second hack.[63] The court also noted that the FTC published a guidebook on cybersecurity with a checklist that formed a sound data security plan which gave the defendant notice of the FTC's enforcement plans.[64]

In 2018, the Eleventh Circuit upheld the district court's motion to dismiss an FTC enforcement order against the defendant in *LabMD, Inc. v. Federal Trade*

3068 (2005); Nationwide Mortgage Group, Inc. & John D. Eubank, 42 F.T.C. 3104 (2005); Petco Animal Supplies Inc., 32 F.T.C. 3221 (2005); Sunbelt Lending Services, Inc., 42 F.T.C. 3153 (2005); MTS, Inc. et. al., 32 F.T.C. 3209 (2004); Guess?, Inc. & Guess.com, Inc., 22 F.T.C. 3260 (2003); Microsoft Corp., 12 F.T.C. 3240 (2002); Eli Lily & Co., 12 F.T.C. 3214 (2002); Sandra L. Rennert et. al., 992 F.T.C. 3245 (2000). *See also* Kosseff, *supra* note 17, at 815-16.

55. *See* Kosseff, *supra* note 17, at 846.

56. *Compare* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 247 (3d Cir. 2015) (affirming the FTC's authority to bring claims under the "unfairness" prong), *with* LABMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221, 1237 (11th Cir. 2018) (vacating an FTC cease-and-desist order due to the FTC's failure to adequately articulate data security standards).

57. Congress passed the Federal Trade Commission Act in 1914. 15 U.S.C. §§ 41-58 (1914).

58. *See* Ian M. Davis, *Resurrecting Magnuson-Moss Rulemaking: The FTC at a Data Security Crossroads*, 69 EMORY L.J. 781, 812-20 (2020) (arguing the FTC should promulgate a data security rule because it will give the FTC an enforceable data security standard that represents industry consensus); *infra* notes 65-73 and accompanying text.

59. 799 F.3d 236 (3d Cir. 2015).

60. *See id*. at 241.

61. *See id*.

62. *See id*. at 254.

63. *See id*. at 247, 256

64. *See id*.

Commission.[65] The court found the FTC's orders to implement reasonable security methods for protecting consumer information and remake its data-security program unenforceable because the FTC's enforcement action did not order LabMD Inc. (LabMD) to cease an unfair act or practice within the meaning of § 5(a).[66] The crux of the holding centered on the FTC's failure to show an injury or likelihood thereof from LabMD's alleged failure to employ reasonable data security.[67] The court found that the FTC could not prove LabMD's data-security program violated unfair or deceitful commerce practices because there is no meaningful standard for the FTC or courts to enforce what constitutes a "reasonably designed data-security program."[68]

Although the FTC historically regulated through enforcement orders,[69] in July 2021, FTC Commissioners approved changes that make rulemaking proceedings less burdensome.[70] In October 2021, the FTC updated its Safeguard Rules to require specific cybersecurity safeguards such as limiting who can access consumer data and using encryption to secure that data.[71] Despite the FTC's recent rulemaking initiatives, the FTC's authority only extends civil penalties against for-profit companies.[72] The FTC's Criminal Liaison Unit works with the DOJ and other state and federal law enforcement offices for criminal consumer fraud cases, but the FTC cannot bring criminal charges.[73]

3. Treasury Department.—The Treasury recently expanded its role in cybersecurity by advising against ransomware payments, specifically in cryptocurrency.[74] On September 21, 2021, the Treasury's Office of Foreign Assets Control (OFAC) reinforced its October 2020 efforts[75] to deter ransom payments to cybercriminals on the Specifically Designated Nationals and Blocked Persons List ("SDN List") or any transaction that violated the International

---

65. 894 F.3d 1221, 1226-27 (11th Cir. 2018).

66. *See id*. at 1232 (holding the FTC's order requiring LabMD implement a "reasonable" security program is void for vagueness because the orders were not reasonably definite).

67. *See id*. at 1226-27.

68. *See id*.

69. *See generally* Robert D. Paul, *The FTC's Increased Reliance on Section 13(b) in Court Litigation*, 57 ANTITRUST L.J. 141, 143 (1988) (explaining how the FTC uses enforcement powers in unfair and deceptive practices litigation).

70. *See* 16 C.F.R. § 1 (2021).

71. *See* 16 C.F.R. § 1.25 (2021).

72. *See A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, FED. TRADE COMM'N (May 2021), https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority [perma.cc/T9C5-52M6].

73. 15 U.S.C. § 53 (1914). *See also Criminal Liaison Unit, and Rulemaking Authority*, FED. TRADE COMM'N, https://www.ftc.gov/enforcement/criminal-liaison-unit [perma.cc/7WDJ-Q6PF].

74. *See* Press Release, U.S. Dep't of the Treasury, Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments (Oct. 1, 2020), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf [perma.cc/QU9C-JQLT].

75. *See id*.

Emergency Economic Powers Act[76] (IEEPA).[77] Specifically, OFAC cites its authority under IEEPA and the Trading with the Enemy Act[78] (TWEA) as grounds for civil penalties against ransom payments to actors on the SDN List, other blocked persons, and those covered by country or region embargoes (such as Cuba, the Crimea region of Ukraine, Iran, North Korea, and Syria).[79] OFAC also states it may impose civil penalties for sanction violations under strict liability with an entity's cooperation as grounds for mitigation.[80] In 2021, OFAC released more detailed guidance on complying with sanctions when using cryptocurrency,[81] and the Treasury released a review of its ransomware sanctions program.[82] The sanction report noted emerging challenges to sanction's efficacy, including cybercriminals and pressure on technical infrastructure from growing financial complexity and competing demands.[83]

4. National Institute of Standards and Technology.—By setting cybersecurity standards and best practices, the NIST plays a vital role in assisting other agencies, such as the FTC, SEC, and CISA, in regulating cyber infrastructure.[84] The NIST is a non-regulatory agency, meaning it does not have regulation or enforcement authority within the United States Department of Commerce; however, the NIST has a wide range of technical expertise.[85] The Institute's broad mission is to promote the United States' innovation and industrial competitiveness by advancing standards and technology that enhance economic security and improve quality of life.[86] Congress and the Executive Branch tasked

---

76. 50 U.S.C. § 35 (1977).

77. *See* Press Release, U.S. Dep't of the Treasury, Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments (Sept. 21, 2021), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf [perma.cc/UWE7-Q28A].

78. 50 U.S.C. § 53 (1917).

79. *See* Press Release, *supra* note 77.

80. *See id*.

81. *See* OFFICE OF FOREIGN ASSETS CONTROL, U.S. DEP'T OF THE TREASURY, SANCTIONS COMPLIANCE GUIDANCE FOR THE VIRTUAL CURRENCY INDUSTRY (2021), https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf [perma.cc/22KS-PC3E].

82. *See* U.S. DEP'T OF THE TREASURY, THE TREASURY 2021 SANCTIONS REVIEW (2021), https://home.treasury.gov/system/files/136/Treasury-2021-sanctions-review.pdf [perma.cc/CXR7-9QJV].

83. *See id*. at 2.

84. *See Uses and Benefits of the Framework*, NAT'L INST. STANDARDS & TECH. (Feb. 8, 2021), https://www.nist.gov/cyberframework/online-learning/uses-and-benefits-framework [perma.cc/3A37-DYHF]; *Understanding the NIST Cybersecurity Framework*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/nist-framework [perma.cc/P2QD-HFJB].

85. *See NIST General Information*, NAT'L INST. STANDARDS & TECH. (Dec. 24, 2008), https://www.nist.gov/director/pao/nist-general-information [perma.cc/NZ86-48E4].

86. *See Laws and Regulations*, NAT'L INST. STANDARDS & TECH. (July 29, 2016), https://csrc.nist.gov/topics/laws-and-regulations [perma.cc/J2C7-6GB4]; *see also About NIST*,

the NIST with promulgating standards for technical industries through congressional legislation or executive orders.[87] For example, Biden's Executive Order on Improving the Nation's Cybersecurity[88] requires the NIST to create guidance on security measures for critical software use.[89] Former President Barack Obama's Executive Order on Improving Critical Infrastructure Cybersecurity[90] directed the NIST to work with the DHS to create a cybersecurity framework for reducing risk to critical infrastructures.[91]

5. Department of Homeland Security.—Congress created the DHS through the Homeland Security Act of 2002[92] to protect the United States from foreign and domestic threats in the wake of 9/11.[93] The Department is now the third largest agency in the Executive Cabinet.[94] Given the DHS's broad authority over foreign and domestic threats and cybercrime's international nature, the DHS has some cybersecurity monitoring and internet-regulating (or "securing") powers.[95]

The DHS monitors cybersecurity risk focusing on immediate ransomware threats under the Biden Administration.[96] The DHS, or agencies within the DHS, can also issue security directives when something threatens America's security interests.[97] For example, after the attack on Colonial Pipeline in 2021, the DHS,

---

NAT'L INST. STANDARDS & TECH. (July 10, 2009), https://www.nist.gov/about-nist/our-organization/mission-vision-values [perma.cc/L3RT-PEH9].

87. *See* 15 U.S.C. § 272 (1988). *See also*, *Publications*, NAT'L INST. STANDARDS & TECH., https://csrc.nist.gov/publications [perma.cc/W8H7-Y87L].

88. Exec. Order No. 14028, 86 Fed. Reg. 26,633 (2021).

89. *See id.*; *see also Security Measures for "EO-Critical Software" Use*, NAT'L INST. STANDARDS & TECH. (July 8, 2021), https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/security-measures-eo-critical-software-use-2 [https://perma.cc/UUE5-QR9H].

90. Exec. Order No. 13636, 78 Fed. Reg. 11,737 (Feb. 19, 2013).

91. *See id.*

92. 6 U.S.C. § 1 (2002).

93. *See The Executive Branch*, WHITE HOUSE, https://www.whitehouse.gov/about-the-white-house/our-government/the-executive-branch/ [https://perma.cc/CKM8-BM9R] (last visited Dec. 28, 2021).

94. *See id.*

95. *See, e.g.*, Press Release, Dep't Homeland Sec., DHS Releases Strategic Principles for Securing the Internet of Things (Nov. 15, 2016), https://www.dhs.gov/news/2016/11/15/dhs-releases-strategic-principles-securing-internet-things [https://perma.cc/N73L-VSU6].

96. *See Cybersecurity*, U.S. DEP'T HOMELAND SEC., https://www.dhs.gov/topic/cybersecurity [https://perma.cc/LN93-ABFP] (last visited Dec. 28, 2021) (describing the DHS's cybersecurity initiatives with four ongoing priorities: (1) cementing the resilience of democratic institutions, including the integrity of elections and institutions outside of the executive branch; (2) building back better to strengthen the protection of civilian federal government networks; (3) advancing a risk-based approach to supply chain security and exploring new technologies to increase resilience; and (4) preparing for strategic, on-the-horizon challenges and emerging technology such as the transition to post-quantum encryption algorithms).

97. *See* 6 U.S.C. § 1 (2002); *Department of Homeland Security Management Directives*, DEPT. HOMELAND SEC. (Nov. 25, 2019), https://www.dhs.gov/department-homeland-security-

through the Department's Transportation Security Administration (TSA),[98] issued a security directive requiring TSA designated critical pipelines to implement multiple protections against cyber intrusions.[99] The security directive requires critical pipelines to take three proactive cybersecurity actions: (1) report cybersecurity incidents to the DHS, (2) designate a Cybersecurity Coordinator who is available at all times to coordinate cybersecurity practices with the TSA and CISA, and (3) identify gaps between their activities and TSA recommendations and report the result to the TSA and CISA.[100] In August 20201, the TSA released another security directive for critical pipelines, but the TSA classified that directive.[101]

6. Cybersecurity & Infrastructure Security Agency.—In 2015, through the Cybersecurity Information Sharing Act,[102] Congress mandated the DHS to release guidance helping non-federal and federal entities share cyber threat indicators.[103] In 2018, Congress created the CISA,[104] housed within the DHS, to serve as the nation's cyber risk advisor spanning both private and public sectors.[105]

CISA's cyber threat monitoring and regulatory actions primarily operate with cooperation from private entities.[106] Still, CISA does develop binding operational directives and emergency directives that require action by certain federal

---

management-directives [https://perma.cc/56ZM-DLRN].

98. 49 U.S.C. § 114 (2001).

99. *See* Press Release, Dep't Homeland Sec., DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators (July 20, 2021), https://www.dhs.gov/news/2021/07/20/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators [https://perma.cc/R6ED-TADM].

100. *See* Security Directive Pipeline-2021-01, Transp. Sec. Admin., Enhancing Pipeline Cybersecurity (May 28, 2021), https://s3.documentcloud.org/documents/20791875/security-directive-on-enhancing-pipeline-cybersecurity.pdf [https://perma.cc/XSD4-SNWL].

101. *See* Ratification of Security Directive, 86 Fed. Reg. 54,953 (Aug. 17, 2021).

102. 6 U.S.C. § 6 (2015).

103. *See id*.

104. 6 U.S.C. § 6 (2018).

105. *See About CISA*, CYBERSECURITY INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/about-cisa [https://perma.cc/UXB4-LVA7]; *DHS Public Organizational Chart*, U.S. DEP'T HOMELAND SEC. (Apr. 2, 2021), https://www.dhs.gov/sites/default/files/ publications/21_0402_dhs-organizational-chart.pdf [https://perma.cc/R4Z6-4AYW].

106. *See Critical Infrastructure Cyber Community C³ Voluntary Program*, CYBERSECURITY INFRASTRUCTURE SEC. AGENCY (Jan. 17, 2020), https://www.cisa.gov/ccubedvp [https://perma.cc/A25L-WAVJ]; *Information Sharing and Analysis Organizations (ISAOS)*, CYBERSECURITY INFRASTRUCTURE SECURITY AGENCY, https://www.cisa.gov/information-sharing-and-analysis-organizations-isaos [https://perma.cc/63UY-M4B4]; *Multi-State Information Sharing and Analysis Center*, CTR. FOR INTERNET SECURITY, https://www.cisecurity.org/ms-isac/ [https://perma.cc/V43N-SJWQ]; *Who We Are*, FINANCIAL SERVS. INFO. SHARING & ANALYSIS CTR., https://www.fsisac.com [https://perma.cc/5LFD-FJMB].

agencies.[107] Although CISA has broad administrative subpoena power[108] to gather necessary information for risk analysis, it does not have subpoena power outside the government or explicit enforcement powers like the DHS's TSA.[109] A critic of CISA's current configuration notes that CISA's private participation model relies on voluntary participants reporting security breaches that it may not know happened.[110]

B. Department of Justice

The DOJ, whose jurisdiction includes the FBI, enforces federal laws and prosecutes cybercrimes.[111] In 2014, the DOJ created a cybersecurity unit that serves as a central hub for expert advice and legal guidance regarding how federal statutes impact cybersecurity; however, this unit does not proactively monitor cyber threats.[112] The FBI has dual responsibilities to prevent harm, as part of the United States Intelligence Community (USIC), and enforce federal laws within the DOJ.[113]

Despite the DOJ and FBI's domestic authority, with foreign suspects, the agencies can face enforcement issues if the foreign country committing a cybersecurity violation does not have an extradition treaty with the United States.[114] For example, when the DOJ charged seven international Advanced Persistent Threat 41 ("APT 41") suspects,[115] the suspects in Malaysia, with a

---

107. *See Cybersecurity Directives*, CYBERSECURITY INFRASTRUCTURE SECURITY AGENCY, https://www.cisa.gov/directives [https://perma.cc/M8EK-8R5D].

108. *See CISA Administrative Subpoena*, CYBERSECURITY INFRASTRUCTURE SECURITY AGENCY, https://www.cisa.gov/cisa-administrative-subpoena [https://perma.cc/Z5JH-A775].

109. *Compare* 49 U.S.C. § 114 *with* H.R. Res. 3359, 115th Cong. (2018) (enacted). *See also* Wade H. Atkinson Jr., *A Review of the Trump Administration's National Cyber Strategy*, 5 STUDENT J. INST. WORLD POLS. 35, 55 (2007).

110. *See* Alice M. Porch, *Spoiling for a Fight: Hacking Back with The Active Cyber Defense Certainty*, 65 S.D.L. REV. 467, 474 (2020).

111. *See Organizational Chart*, DEP'T OF JUST., (Oct. 28, 2021) https://www.justice.gov/agencies/chart [https://perma.cc/LEN9-GFJ8].

112. *See Cybersecurity Unit*, DEP'T OF JUST., (June 16, 2021) https://www.justice.gov/criminal-ccips/cybersecurity-unit [https://perma.cc/43DZ-ZQSD].

113. *See Addressing Threats to the Nation's Cybersecurity*, FED. BUREAU INVESTIGATIONS, https://www.fbi.gov/file-repository/addressing-threats-to-the-nations-cybersecurity-1.pdf/view [https://perma.cc/2LSP-B4X9].

114. *See* Jonathan Masters, *What is Extradition?*, COUNCIL ON FOREIGN REL. (Jan. 8, 2020), https://www.cfr.org/backgrounder/what-extradition [https://perma.cc/4Q7C-AQET] (describing how the United States does have extradition treaties with dozens of countries, including China, Iran, North Korea, and Russia, as well as many African, Middle Eastern, and formerly Soviet countries).

115. *See* Press Release 20-942, Dep't of Just., Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection with Computer Intrusion Campaigns Against More Than 100 Victims Globally (Sept. 16, 2020), https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer [https://perma.cc/S3SQ-CZRF];

United States extradition treaty, were extradited to the United States, whereas the suspects in a country without an extradition treaty with the United States, China, remain fugitives.[116] Given these extradition problems, the FBI's general cybersecurity strategy is to impose risk and consequences on cyber adversaries,[117] despite the charges against APT 41 likely not quashing the state-sponsored organization.[118] Despite these enforcement hurdles, in October 2021, the DOJ expanded its cyberlaw enforcement initiative domestically to government contractors who receive federal funds.[119]

C. Biden Administration's Approach to Cybersecurity

After inheriting the SolarWinds Hack's aftermath, President Biden had to address the Colonial Pipeline Hack only a few months after assuming office.[120] On May 12, 2021, less than one week after the Colonial Pipeline Hack, the Biden Administration issued an executive order for improving the nation's cybersecurity.[121] The executive order establishes breach requirements for internet technology service providers, various security protocols for the federal government, a Cyber Safety Review Board, and a standardized playbook for cybersecurity vulnerability and response procedures.[122]

APT 41 Group, FED. BUREAU OF INVESTIGATIONS, https://www.fbi.gov/wanted/cyber/apt-41-group [https://perma.cc/HU7V-VMPP]. APT 41, also known as Double Dragon, is a China-sponsored espionage and cybercrime operation that blurs the lines between state-sponsored and commercial cybercrime. *See generally* Special Report, *Double Dragon: APT 41, A Dual Espionage and Cyber Crime Operation*, FIREEYE 5 (2019), https://content.fireeye.com/apt-41/rpt-apt41/.

116. *See APT 41 Group*, *supra* note 115.

117. *See* Press Release, Fed. Bureau of Investigations, FBI Strategy Addresses Evolving Cyber Threat (Sept. 16, 2020), https://www.fbi.gov/news/stories/wray-announces-fbi-cyber-strategy-at-cisa-summit-091620 [https://perma.cc/YD7K-QAT5].

118. *See* Thomas Brewster, *Are the FBI's 'Most Wanted' Chinese Spies Hacking the Airline Industry*, FORBES (June 10, 2021), https://www.forbes.com/sites/thomasbrewster/2021/06/10/are-the-fbis-most-wanted-chinese-spies-hacking-the-airline-industry/ [https://perma.cc/9QB2-568F] (reporting on cybersecurity's firm analysis that APT 41 is likely the culprit of an attack against Air India).

119. *See* Press Release 21-971, Dep't of Just., Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative (Oct. 6, 2020), https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative [https://perma.cc/KH2N-UY6E].

120. *See* Romo, *supra* note 9; Temple-Raston, *supra* note 5.

121. *See* Exec. Order No. 14028, 86 Fed. Reg. 26,633 (May 12, 2021); Press Release, White House, Executive Order on Improving the Nation's Cybersecurity (May 12, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/[https://perma.cc/89RK5RND].

122. *See id*.

Speaking in June 2021, with Russian President Vladimir Putin,[123] President Biden stated that "critical infrastructures should be off limits to attack . . . ."[124] In addition, President Biden declared that he would not tolerate attempts to violate the United States' democracy.[125] The meeting ended with the two leaders agreeing to task experts in both countries to determine the parameters of cybersecurity related actions and follow up on specific cases that originate in the United States or Russia.[126] While the House Intelligence Chair was encouraged by Biden's explicit statements and promise that targeting critical infrastructure would have real consequences,[127] skeptics believe that any agreement Putin may make is not credible and, at worst, could give Russia a roadmap for attacking industries that cause the most harm to the United States.[128]

On July 28, 2021, the Biden Administration released a national security memo focused on improving cybersecurity for critical infrastructure control systems that directs the NIST to develop cybersecurity performance goals to drive effective practices and controls in collaboration with the Department of Commerce.[129] NIST has also noted it will play a role in that collaboration.[130]

---

123. *See* Press Conference, White House, Remarks by President Biden in Press Conference (June 16, 2021), https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/06/16/remarks-by-president-biden-in-press-conference-4/ [https://perma.cc/4T2T-CJAL].

124. *See id*. Biden's list of "critical infrastructures" included water, food and agriculture, transportation, information technology, nuclear materials, chemical, commercial, communication, some manufacturing, dams, emergency services, energy, financial, government facilities, healthcare, and defense industry sectors. *Id*. *See also Critical Infrastructure Sectors*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, (Oct. 21, 2020) https://www.cisa.gov/critical-infrastructure-sectors [https:/perma.cc/5NRU-UJTM].

125. *See* Press Conference, *supra* note 123.

126. *See id*.

127. *See* John Dickerson, *Transcript: Representative Adam Schiff on "Face the Nation"*, CBS NEWS (June 20, 2021), https://www.cbsnews.com/news/transcript-representative-adam-schiff-on-face-the-nation-june-20-2021/[https://perma.cc/5T88-KCRL].

128. *See* Editorial Board, *Putin Tests Biden's Cyber Vow*, WALL ST. J. (July 7, 2021), https://www.wsj.com/articles/putin-tests-bidens-cyber-vow-11625676711 [https://perma.cc/ZA9W-R8RY]; Houston Keene & Evie Fordham, *Biden's "Off-Limits" List for Russian Cyberattacks Criticized as "Green Light" to Target Everything Else*, FOX NEWS (June 18, 2021), https://www.foxnews.com/politics/biden-putin-russian-cyberattacks-list-16-off-limits-criticism [https://perma.cc/ZFZ5-NPAU]; Martin Matishak, *Biden's Vow of Digital Reprisals Against Russia Draws Skepticism*, POLITICO (July 16, 2021), https://www.politico.com/news/2021/06/16/biden-cyber-russia-494957 [https://perma.cc/T8ZH-NG4L]. In late September 2021, after Biden and Putin's discussion, NEW Cooperative Inc., an Iowa-based farm service provider took its system offline to manage a cybersecurity threat. *See* Karl Plume & Christopher Bing, *Iowa Farm Services Firm: Systems Offline Due to Cybersecurity Incident*, REUTERS (Sept. 20, 2021), https://www.reuters.com/technology/iowa-farm-services-company-reports-cybersecurity-incident-2021-09-20/ [https://perma.cc/PV6K-D4MY]. Shortly thereafter, BlackMatter, a Russian-speaking cybercriminal group, announced they stole data from the service provider. *See id*.

129. *See* Press Release, White House, National Security Memorandum on Improving

In late August 2021, the Biden Administration continued their cybersecurity efforts by meeting with various private entities with high cybersecurity stakes, including Amazon, Google, IBM, Microsoft, Apple, JPMorgan Chase, and cyber insurance companies, to discuss developing "whole-of-[the]-nation" cybersecurity.[131] While the Biden Administration did not define the phrase "whole-of-nation," presumably this effort includes the private sector collaborating with the government on national cybersecurity measures rather than focusing on specific industries or types of infrastructure.[132] During this meeting, many attending companies made voluntary promises, such as training 150,000 cybersecurity professionals and committing ten million dollars to strengthen the company's product and supply chain cybersecurity.[133]

D. Proposed Federal Cybersecurity Regulation

As cyberattacks increase, more congresspeople have shown interest in passing new cybersecurity laws.[134] The proposed Active Cyber Defense Certainty Act[135] (ACDC) would bring back the President Barak Obama-era cybersecurity law that allows companies to trace, or attribute, cyber hacks to their culprit using otherwise illegal actions.[136] Notable drawbacks of the ACDC are that the law

---

Cybersecurity for Critical Infrastructure Control Systems (July 28, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/[https://perma.cc/UM9L-UHWV]; Press Release, Nat'l Inst. of Standards & Tech., NIST & DHS Developing Cybersecurity Performance Goals for Critical Infrastructure Control Systems (July 29, 2021) [hereinafter NIST & DHS Goals], https://www.nist.gov/news-events/news/2021/07/white-house-national-security-memo-issued-nist-dhs-developing-cybersecurity [https://perma.cc/9ZM9-V723].

130. *See* NIST & DHS Goals, *supra* note 129.

131. *See* Press Release, The White House, Fact Sheet: Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation's Cybersecurity (Aug. 25, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/25/fact-sheet-biden-administration-and-private-sector-leaders-announce-ambitious-initiatives-to-bolster-the-nations-cybersecurity/ [perma.cc/R8EE-97SB].

132. The idea of a "whole-of-nation" cybersecurity approach has existed since the Obama Administration. *See* Exec. Order No. 13718, 3 Fed. Reg. 13,718 (Feb. 9, 2016).

133. *See* Cat Zakrzewski et al., *Biden Tells Top CEOs at White House Summit to Step Up on Cybersecurity*, WASH. POST (Aug. 25, 2021), https://www.washingtonpost.com/technology/2021/08/25/white-house-cybersecurity-summit-apple-amazon/ [https://perma.cc/RJP7-WTP2] (describing the outcome of President Biden's meeting with private sector industry leaders).

134. *See* Cynthia Brumfield, *Eighteen New Cybersecurity Bills Introduced as US Congressional Interest Heats Up*, CSO (July 27, 2021), https://www.csoonline.com/article/3626908/18-new-cybersecurity-bills-introduced-as-us-congressional-interest-heats-up.html [perma.cc/Y7SW-ZMUE].

135. H.R. 3270, 116th Cong. (2019).

136. *See* Porch, *supra* note 110, at 477.

would not provide ex ante cybersecurity defense mechanisms and may further convolute already complicated investigations by corrupting evidence.[137] Furthermore, this strategy of attributing a hack or finger-pointing may have less societal value than building a resilient cyber defense because foreign actors are unlikely to be extradited to the United States.[138] In addition, false cybersecurity accusations could harm foreign policy initiatives and goals.[139]

E. Previously Offered Solutions

Previously offered improvements to domestic cyber-defense include: (1) sanctioning ransomware payments (presumably to deter cyberattacks by prohibiting a direct monetary reward),[140] (2) creating a federal cybersecurity insurance policy,[141] and (3) treating data as an abnormally dangerous activity.[142] Though these solutions aim to mitigate harm from cyberattacks, they do not include centralized threat-monitoring or focus on citizen-led cyber regulation through agency rulemaking.[143]

These proposals do not rectify the underlying insufficiencies in current piecemeal federal cybersecurity regulation.[144] Instead, the proposals perpetuate sectoral and public versus private division in cybersecurity, not ex ante "whole-of-nation" cybersecurity that streamlines cyber threat monitoring and regulations.[145]

The lack of cohesion in current and proposed cyber regulations and laws hinders the nation's cybersecurity because, as the SolarWinds Hack demonstrates, cyber threats can migrate across infrastructures and industries.[146] In addition to

---

137. *See id*. at 478.

138. *See id*. at 488.

139. *See id.*

140. *See* Ra'na Heidari, *I Got Hit with Ransomware. Now What?*, 33 S.C. LAW. 47, 48 (2021) (describing the Treasury's approach to sanctioning ransomware payments through civil penalties); *supra* notes 74-82 and accompanying text.

141. *See generally* Angard Chopra, *Cyberattack—Intangible Damages in a Virtual World: Property Insurance Companies Declare War on Cyber-Attack Insurance Claims*, 82 OHIO ST. L.J. 121, 158-61 (2021) (arguing a federal cybersecurity program would work as an ex-ante prophylactic against litigation).

142. *See generally* Jordan Glassman, *Too Dangerous to Exist: Holding Comprised Internet Platforms Strictly Liable Under the Doctrine of Abnormally Dangerous Activities*, 22 N.C. J. L. & TECH. 293, 315-19 (2020) (arguing that internet platforms create foreseeable highly significant risks that are not preventable with reasonable care with complex liability).

143. *See supra* notes 17-32 and accompanying text.

144. *See id.*

145. *See infra* Part II.

146. *See supra* notes 5-6 and accompanying text. *See generally* Martin Borrett et al., *How is Cyber Threat Evolving and What Do Organizations Need to Consider?*, 7 J. BUS. CONTINUITY & EMERGENCY PLAN. 163 (2014) (discussing the proliferation of across industries security breaches); Rob Sloan, *Which Industries Aren't Ready For a Cyberattack?*, WALL ST. J. (June 21, 2020),

not streamlining regulation and dichotomizing data protection from cybersecurity, proposed and current cyberlaw focus on attributing a hack to its culprit and generally rely on business collaboration that is not easily reviewable by citizens or interest groups.[147]

1. Sanctioning Ransomware Payments.—The Treasury sanctions ransomware payments to specific identified criminal organizations.[148] This effort is part of Biden's integrated (whole—of—the—nation) cybersecurity effort,[149] but the Treasury's sanctions may deter cyberattacks less than anticipated and not enhance proactive cyber defense and security.[150] First, by the time a cybercriminal requests ransomware from an organization, the hacker has already breached the organization's cyber infrastructure.[151] After an attack, the organization can only: (1) pay the ransom in the hopes of regaining access, (2) attempt to restore control through backups, or (3) pray a decryption key is available.[152] The sanctions also assume cybercriminals are only, or at least primarily, financially motivated, which is likely false given the surge in state-sponsored cyberattacks.[153] Lastly, the

---

https://www.wsj.com/articles/the-industries-most-vulnerable-to-cyberattacksand-why-11592786160 [perma.cc/NT9E-VHFV] (reporting on cyber threats across companies' industries and sizes).

147. *See infra* Part II; *see also* Mark Hilliard, *Less Fear and More Transparency Key to Fighting Cybercrime*, IRISH TIMES (Nov. 15, 2018), https://www.irishtimes.com/business/ technology/less-fear-and-more-transparency-key-to-fighting-cybercrime-1.3692135 [perma.cc/NDT5-244K] (reporting on cybersecurity officials that argue transparency, rather than secrecy and mystique, allows potential cyber victims to protect themselves); Itzik Kotler, *Transparency, Trust and Cybersecurity's Long Game*, FORBES (July 14, 2020), https://www.forbes.com/sites/forbestech council/2020/07/14/transparency-trust-and-cybersecuritys-long-game/ [https://perma.cc/327A-D2KX] (discussing what would happen if cybersecurity did not operate under a veil of secrecy and transparency foster greater knowledge, innovation, and awareness); *Welcome to Transparency in Cybersecurity*, TRANSPARENCY CYBERSECURITY, https://transparency incyber.org [perma.cc/PJ93-KWXD] (stating transparency in cybersecurity benefits both consumers and industry).

148. *See supra* notes 75-83 and accompanying text.

149. *See* Press Release, White House, Fact Sheet: Ongoing Public U.S. Efforts to Counter Ransomware (Oct. 13, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware/ [perma.cc/LQW5-8HVJ].

150. Despite the Treasury's sanctions beginning in October 2020, ransomware cyberattacks continue rising. *See, e.g.*, Ian Talley, *Suspected Ransomware Payments Nearly Doubled This Year, Treasury Says*, WALL ST. J. (Oct. 15, 2021), https://www.wsj.com/articles/suspected-ransomware-payments-for-first-half-of-2021-total-590-million-11634308503 [perma.cc/Y4JA-VSTR].

151. *See* Heidari, *supra* note 140, at 48.

152. *See id.*

153. *See generally* Alan Rappeport et. al., *The Biden Administration is Combating Ransomware with a Crackdown on Cryptocurrency Payments*, N.Y. TIMES (Sept. 21, 2021), https://www.nytimes.com/2021/09/21/us/politics/treasury-department-combating-ransomware-cryptocurrency.html [perma.cc/U5VR-ABHD] (reporting the FBI's deputy perspective that Russian government cracked down on ransomware actors).

Treasury's sanctions may have unintended consequences.[154] For instance, if the Treasury imposes civil monetary sanctions rather than criminal sanctions, the Treasury's policies may increase the cost of cybercrime to United States organizations and individuals since attacked entities may decide to pay the ransom *and* sanctions rather than comply with the Treasury's ransomware policies.[155]

2. Government Cybersecurity Insurance.—Another proposed improvement involves creating a federal cybersecurity insurance policy similar to post-World War Two war risk insurance policies.[156] This insurance program migrates cybersecurity risk from the private insurance sector to the government through war exclusion clauses in insurance contracts.[157] Potential benefits of a federal cyber insurance program include providing the government, and security community specifically, with more information regarding cyberattack methods that may spur cyber defense innovation.[158] Given this potential benefit, creating federal cyber insurance could, in the long term, improve the nation's defensive cybersecurity.[159] However, it could also create or exacerbate market inefficiencies and stifle cybersecurity innovation as insulating companies from their direct cyber risks may disincentivize private entities from developing cybersecurity methods.[160] Furthermore, implementing this program without mandatory cybersecurity reporting requirements could make it challenging to calculate systemic risk.[161] In

---

154. *See generally* Daniel Fried & Brian O'Toole, *US Leaders Laid Down Solid and Sensible Sanctions Policy. Now They Need to Follow Through*, ATLANTIC COUNCIL (Oct. 20, 2021), https://www.atlanticcouncil.org/blogs/new-atlanticist/us-leaders-laid-down-solid-and-sensible-sanctions-policy-now-they-need-to-follow-through/ [perma.cc/BX5W-A6V3] (explaining that successful sanctions depend on clear policy objectives and should incorporate multilateral coordination).

155. *See id*. (stating sanctions are not immune from misapplication or abuse).

156. *See* Chopra, *supra* note 141, at 129-32.

157. *See id*. at 125.

158. *See id*. at 161.

159. *See id*.

160. *See generally* INTERNET POL'Y TASK FORCE, DEP'T OF COM., CYBERSECURITY, INNOVATION AND THE INTERNET ECONOMY (2011), https://www.nist.gov/system/files/documents/itl/Cybersecurity_Green-Paper_FinalVersion.pdf [perma.cc/P73L-V49H] (recommending a new cybersecurity framework for non-critical infrastructure companies); James Andrew Lewis, *Linking National Security and Innovation: Part 1*, CTR. FOR STRATEGIC & INT'L STUD. (Apr. 7, 2021), https://www.csis.org/analysis/linking-national-security-and-innovation-part-1 [perma.cc/V6JS-QKJ7] (explaining how companies focus on returns from innovation disincentivizes security development).

161. *See generally* Christina Ayiotis et. al., *Key Cyber Issues and Recommendations: A Way Forward*, ARMED FORCES COMM. & ELECTRONICS ASS'N (Dec. 2016), https://www.afcea.org/content/afcea-whole-nation-cybersecurity-approach-needed [perma.cc/H597-2G4S] (identifying three cybersecurity needs: (1) approaching cybersecurity with a diplomatic and strategic perspective, (2) improving and expanding the public-private cooperative ecosystem, and (3) developing cybersecurity work force); Jonathan Welburn & Aaron Strong, *Systemic Cyber Risk and Aggregate*

addition, cybercriminals, especially state-sponsored cybercriminals, could exploit the insurance program if they know that the companies are insured and the government is financially liable.[162]

3. Cyber Infrastructure as an Abnormally Dangerous Activity—A third suggested cybersecurity law improvement includes treating some "dangerous" internet platforms strictly liable for data breaches or cyber hacks to their platforms under an abnormally dangerous activity theory.[163] Holding these platforms strictly liable may incentivize private entities to guard their infrastructure proactively,[164] but, given that no cyber platform or infrastructure can be entirely secure, it may unfairly penalize companies that suffer a cyberattack despite taking reasonable care.[165] Under this proposal, cyber defense remains siloed and is even narrower than the "critical infrastructure" approach because it is entity, not industry, specific.[166]

II. CURRENT AND PROPOSED CYBER REGULATION INSUFFICIENCIES

Like the federal security community before the 9/11 terrorist attacks,[167] the hodgepodge mix of state and federal industry-specific data privacy and security legislation does not provide efficient sharing of threat indicators,[168] maximize certainty[169] and security,[170] or account for the connection between data privacy

---

Impacts, RAND CORP. (Feb. 18, 2021), https://www.rand.org/pubs/external_publications/EP68520.html [perma.cc/2XHM-YVLZ] (explaining their quantitative model of cascading, systemic cyber risks across sectors which complicate businesses' cyber risks and costs assessments); Bob Zukis, *Some Vital Lessons in How Systemic Risk Is Changing Cybersecurity*, FORBES (Sept. 2, 2021), https://www.forbes.com/sites/bobzukis/2021/09/02/some-vital-lessons-in-how-systemic-risk-is-changing-cybersecurity/ [https://perma.cc/8KK4-NXPR] (describing how sophisticated hackers pinpoint systemic risk in complex, across sector systems to bring an entire system to a standstill).

162. *See* Jeffery L. Vagle, *Cybersecurity and Moral Hazard*, 22 STAN. TECH. L. REV. 71, 85-97 (2020) (explaining the unique moral hazard issues internet technology presents).

163. *See* Glassman, *supra* note 142, at 315.

164. *See id*. at 318.

165. *See id*. at 315.

166. *See id*. at 318.

167. *Cf.* Kosseff, *supra* note 17, at 815-16.

168. *See* Tarun Chaudhary et al., *Patchwork of Confusion: The Cybersecurity Coordination Problem*, 4 J. CYBERSECURITY 1, 2-4 (2018) (explaining how patchwork federal regulation creates confusion and competition among cybersecurity agencies).

169. *See* Porch, *supra* note 110, at 477.

170. *See generally* James Andrew Lewis, *Economic Impact of Cybercrime*, CTR. FOR STRATEGIC & INT'L STUD. (Feb. 21, 2018), https://www.csis.org/analysis/economic-impact-cybercrime [perma.cc/U68L-6MCP] (explaining cybercrimes remains far too easy and profitable since users do not use basic protective measures and many technology products lack adequate defenses).

breaches and cyberattacks.[171] Thus, since current federal cybersecurity lacks centralized authority, pre-and-post-9/11 national security legislation, like the Patriot Act[172] and Homeland Security Act,[173] and resulting federal agency changes,[174] like creating CISA,[175] provide a model for effective cybersecurity across the nation.

The 9/11 attacks illuminated weaknesses in the federal security community, specifically the lack of consolidated information and threat oversight.[176] The Central Intelligence Agency knew of the imminent attack and shared that information with the National Security Agency and FBI, but no one working on these late leads in the summer of 2001 connected the case in his or her in-box to the threat reports agitating senior officials and being briefed to the President.[177] After the avoidable 9/11 attacks, Congress created the DHS,[178] and President George W. Bush created the National Counterterrorism Center.[179] These agencies proactively share information for terrorism threat monitoring and coordinating national strategies.[180]

The main problem with current cybersecurity regulation is the lack of cohesion among agencies and a centralized rulemaking authority.[181] Despite increasing cyber threats, the sectoral cybersecurity approach mimics the pre-9/11 security communities' disorganization, inhibiting robust national defense and response procedures.[182]

---

171. *See* Jon M. Garon, *The Empires Strike Back: Reassertion of Territorial Regulation in Cyberspace*, 3 TEX. J. L. & TECH. 1, 36-37 (2020) (explaining that malicious or criminal attacks now account for forty-eight percent of data breaches, making the need to respond to these outward attacks an even larger priority).

172. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107-56, 86 Stat. 1116.

173. 6 U.S.C. § 1 (2002); *see also* accompanying text of note 92.

174. *See generally* Eric Holder, *We're Safer Post-9/11*, DOJ ARCHIVES, (Sep. 8, 2011), https://www.justice.gov/archives/opa/blog/were-safer-post-911 [https://perma.cc/88PL-7P8Q] (explaining how new centralized federal agencies developed a robust information-sharing environment that makes the United States safer than pre-9/11 national security).

175. *Supra* notes 102-05 and accompanying text.

176. *See* THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 254 (2004), https://govinfo.library.unt.edu/911/report/911Report.pdf [perma.cc./FC73-G79K] (describing how the intelligence system was "blinking red" before the 9/11 attacks).

177. *See id*.

178. *The Executive Branch*, *supra* note 93.

179. Exec. Order No. 13354, 3 C.F.R. 13354 (Aug. 27, 2004).

180. *See generally* DEP'T OF HOMELAND SECURITY, NATIONAL STRATEGY FOR INFORMATION SHARING (2012), https://www.dhs.gov/sites/default/files/publications/15_1026_NSI_National-Strategy-Information-Sharing-Safeguarding.pdf; DEP'T OF HOMELAND SECURITY, NATIONAL STRATEGY FOR INFORMATION SHARING (2007), https://www.dhs.gov/sites/default/files/publications/10_0924_NSI_National-Strategy-Information-Sharing.pdf.

181. *See supra* notes 17-18.

182. *See supra* notes 167-71.

Three core themes in federal cybersecurity obstruct the nation's overall cyber defense.[183] As discussed, current cybersecurity regulation lacks a centralized regulatory body that can enforce nationwide standards.[184] Separating data privacy from cybersecurity exacerbates the information-sharing problems that result from non-centralized threat monitoring.[185] Additionally, cybersecurity regulation focuses on private sectors and attributing attacks.[186] Relying on business cooperation makes monitoring threats harder[187] and does not include non-profit entities, like hospitals and schools, and individuals in decision-making.[188] Lastly, attributing cyberattacks and relying on private sector cooperation does not maximize *ex ante* cyber infrastructure defense[189] and, given extradition problems, may not lead to enforcement given extradition problems.[190]

As discussed in Section I.A, current cybersecurity regulation lacks a centralized regulatory body that can enforce nationwide standards.[191] Section II.A discusses the issues the lack of centralized cybersecurity authority presents. Section II.B discusses how relying on business cooperation makes monitoring threats more difficult and does not include information and knowledge from non-profit entities, like hospitals and schools, and individuals in decision-making. Section II.C of this Article discusses issues arising from focusing on attribution rather than ex ante defense.

A. Lack of Centralization in Federal Cybersecurity

The current hodgepodge of cybersecurity laws in the United States focuses on specific industries or interests.[192] For instance, the SEC's authority only

---

183. *See infra* Sections II.A-C.

184. *See supra* notes 18-26 and accompanying text.

185. *See* Garon, *supra* note 171 and accompanying text; *infra* note 201 and accompanying text.

186. *See supra* Sections I.A-E.

187. Larry Clinton, *A Relationship on the Rocks: Industry—Government Partnership for Cyber Defense*, 4 J. OF STRATEGIC SECURITY 97, 108 (2011); Amitai Etzioni, *Cybersecurity in the Private Sector*, 28 ISSUES SCI. & TECH. 58, 59-62 (2011).

188. *See generally* Emma Osborn & Andrew Simpson, Small-Scale Cyber Security, 2015 IEEE 2ND INTERNATIONAL CONFERENCE ON CYBER SECURITY AND CLOUD COMPUTING (2015) (arguing for greater attention to small scale internet technology users); Jason Thomas, *Individual Cyber Security: Empowering Employees to Resist Spear Phishing to Prevent Identity Theft and Ransomware Attacks*, 12 INT'L J. BUS. MGMT. 1, 1-2 (2018) (explaining the prevalence and consequences of cyberattacks targeting individuals).

189. Johannes M. Bauer & Michel J.G. van Eeten, *Cybersecurity: Stakeholder Incentives, Externalities, and Policy Options*, 33 TELECOMM. POL'Y 706, 719 (2009); BRIAN M. MAZANEC & BRADLEY A. THAYER, CONTINUING EFFORTS TO IMPROVE CYBER FORENSICS AND BOLSTER DEFENSES 57-63 (1st ed. 2015).

190. *See supra* notes 114-18 and accompanying text.

191. *See supra* notes 18-23 and accompanying text.

192. *See supra* notes 18-19 and accompanying text.

extends to financial services companies.[193] And, the FTC focuses on consumer protection even though it is the closest thing the United States has to a central cybersecurity regulatory agency.[194] Though CISA centralizes some information, it also follows a sectoral approach, focusing on federal agencies and "critical infrastructures."[195] Given CISA does not have rulemaking authority beyond federal agencies or enforcement powers, the Agency cannot regulate or efficiently protect the entire nation, including the private sector, government, non-profit organizations, and individuals.[196]

As the 9/11 terrorist attacks demonstrate, non-centralized threat monitoring obstructs robust national defense because threat patterns are harder to observe when monitors do not have all the available information.[197] Any cybersecurity program that does not facilitate centralized reporting/threat-monitoring across sectors cannot adequately account for systemic risks because affected companies will fall outside the monitoring purview.[198] For instance, had a centralized cybersecurity agency regulated companies' cyber infrastructures, threat monitoring, and reporting more systematically, CISA may have discovered the SolarWinds Hack earlier and saved "critical infrastructures" far sooner in the process, rather than six months after the initial attack when an infected company discovered and reported the hack.[199] Similarly, a centralized cybersecurity agency could implement cybersecurity regulations, like multi-factor authentication, for virtual private networks and other cyber infrastructure access mechanisms, including requiring companies store information on domestic servers with specific virtual and physical infrastructure protection, which could have prevented the Colonial Pipeline Hack.[200]

---

193. *See supra* note 51 and accompanying text.

194. *See supra* notes 52-56 and accompanying text.

195. *See, e.g., Cybersecurity Directives*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, https://www.cisa.gov/directives [perma.cc/4GVB-K4YG]; *Infrastructure Security*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, https://www.cisa.gov/infrastructure-security [perma.cc/D33S-MQ5Y].

196. Tonya Riley & Aaron Schaffer, *The Cybersecurity 202: Lawmakers Want Greater Resources, Authorities for CISA to Protect Critical Infrastructure*, WASH. POST (May 5, 2021), https://www.washingtonpost.com/politics/2021/05/05/cybersecurity-202-lawmakers-want-greater-resources-authorities-cisa-protect-critical-infrastructure/ [perma.cc/LYF9-76KY]; *supra* notes 108-10 and accompanying text.

197. *See supra* notes 167-80 and accompanying text.

198. *See id*.

199. Letter from Brandon Wales, Acting Director, CISA, to Rob Wyden, Senator, U.S. Cong. (June 3, 2021), https://www.documentcloud.org/documents/20969575-wyden_response_signed [perma.cc/CYB8-9ULK]; Raphael Satter, *SolarWinds Hackers Could Have Been Waylaid by Simple Countermeasure—US Officials*, REUTERS (June 21, 2021, 8:00 PM), https://www.reuters.com/technology/solarwinds-hackers-could-have-been-waylaid-by-simple-countermeasure-us-officials-2021-06-21/ [https://[erma.cc/BPN-UUU3].

200. *Threats to Critical Infrastructure: Examining the Colonial Pipeline Cyber Attack: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affs.*, 118th Cong. (2021) (statement of

In addition, current cybersecurity and data privacy initiatives do not incorporate their interdependencies.[201] This dichotomization hinders both cybersecurity and data privacy because stealing data may motivate cyberattacks, which often cause data breaches.[202] Segregating cybersecurity from data privacy ignores their intersection and effects on each other, which inhibits centralized threat analysis and fast, coordinated cyberattack and data privacy breach mitigation.[203]

B. Private Sector Self-Regulation and Cooperation

Though the Biden Administration shifted focus from "critical infrastructures" to "whole-of-nation" cybersecurity, both approaches generally focus on private industry participation and cooperation, not agency rulemaking.[204] While businesses suffer cyberattacks, the harm is not limited to these entities and their clients, customers, and users.[205] The FTC and SEC regulate private companies,[206] but cybercriminals also attack individuals and non-profit organizations, like hospitals.[207] The focus on sector-specific regulation and industry cooperation does

---

Joseph Blount, President and CEO, Colonial Pipeline); Stephanie Kelly & Jessica Resnick-ault, *One Password Allowed Hackers to Disrupt Colonial Pipeline, CEO Tells Senators*, REUTERS (June 8, 2021), https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/ [https://perma.cc/N6JU-PY4T].

201. Andrew Burt, *Privacy and Cybersecurity Are Converging. Here's Why That Matters for People and for Companies*, HARV. BUS. REV. (Jan. 3, 2019), https://hbr.org/2019/01/privacy-and-cybersecurity-are-converging-heres-why-that-matters-for-people-and-for-companies [perma.cc/9D3Y-6GNT]; Gabe Morazan, *Digital Privacy vs. Security Is a False Dichotomy*, CMSWIRE (Oct. 23, 2019), https://www.cmswire.com/digital-experience/digital-privacy-vs-security-is-a-false-dichotomy/ [perma.cc/844V-UJLQ].

202. *See* Garon, *supra* note 171.

203. *See id.*

204. Maggie Miller, *Biden 'Confident' in the Nation's Cybersecurity Efforts as Cybersecurity Awareness Month Begins*, THE HILL (Oct. 1, 2021), https://thehill.com/policy/cybersecurity/574933-biden-confident-in-the-nations-cybersecurity-efforts-as-cybersecurity [perma.cc/FP9V-ZTY2].

205. *See supra* notes 15, 188 and accompanying text. *See generally*, Ioannis Agrafiotis et al., *A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate*, 4 J. CYBERSECURITY 1 (2018) (explaining a taxonomy of cyber-harms including physical or digital harm, economic harm, psychological harm, reputation harm, and social and society harm).

206. *See supra* notes 42-53 and accompanying text.

207. FED. BUREAU OF INVESTIGATIONS, 2020 INTERNET CRIME REPORT (Mar. 17, 2021), https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf; Molly Click, *Cyberattacks on Health Care Are Rising—But Many Hospitals Aren't Prepared*, DISCOVER MAG. (Sept. 13, 2021, 7:00 PM), https://www.discovermagazine.com/technology/cyberattacks-on-health-care-are-rising-but-many-hospitals-arent-prepared [perma.cc/W8Y3-8HZW]; Emily Skahill & Darrell M. West, *Why Hospitals and Healthcare Organizations Need to Take Cybersecurity More Seriously*, BROOKINGS INST. (Aug. 9, 2021), https://www.brookings.edu/blog/techtank/2021/08/09/why-

not incorporate individuals' and smaller companies' perspectives.[208] Not including all perspectives limits agency expertise and transparency because, without rulemaking, agencies do not seek as much information as possible to inform their actions as possible and provide abundantly clear notice.[209] Expertise, transparency, and notice are parts of the information sharing and knowledge transfers that agencies need for efficient regulation because it allows the regulator and regulated to identify vulnerabilities and pool resources for collaborative problem solving.[210] Relying on market or cooperation based cybersecurity does not ensure optimal information sharing and knowledge transfers because sharing cyber threats or attacks may affect the company's profits, and companies may not have the information and expertise necessary to assess cyber threats outside the individual company's cyber infrastructure systems.[211]

C. Focus on Attributing Cyberattacks

The Treasury's ransomware sanctions, DOJ's enforcement, including the FBI's participation, and ACDC focus on the attacker's identity.[212] Attributing a hack to its culprit could theoretically deter future attacks, but identification does not provide actual, ex ante cyber defense because attribution or ransomware payment sanctions do not secure cyber infrastructures' attack susceptibility or foster threat and attack reporting.[213]

Specifically, the ACDC may disincentivize immediate threat or hack reporting from attacked entities if the entity knows it is legally authorized to "hack back" the culprit.[214] Also, under the ACDC, an attacked entity may further

---

hospitals-and-healthcare-organizations-need-to-take-cybersecurity-more-seriously/ [perma.cc/M765-3E88].

208. Kiersten E. Todt, *Small Businesses Barely Survive Cyberattacks—the US Must Help to Secure Them*, THE HILL (May 7, 2021), https://thehill.com/opinion/cybersecurity/552296-small-businesses-barely-survive-cyber-attacks-the-us-must-help-to [perma.cc/ST82-7SMX].

209. MICHAEL SANT' AMBROGIO & GLEN STASZEWSKI, PUBLIC ENGAGEMENT IN RULEMAKING 1-7 (2018), https://www.acus.gov/sites/default/files/documents/Public%20Engagement%20in%20Rulemaking%20Final%20Report.pdf; Cary Coglianese et al., *Transparency and Public Participation in the Federal Rulemaking Process: Recommendations for the New Administration*, 77 GEO. WASH. L. REV. 924, 926-30 (2009).

210. Eldar Haber & Tal Zarsky, *Cybersecurity for Infrastructure: A Critical Analysis*, 44 FL. ST. U. L. REV. 515, 573 (2017).

211. *See id*. at 544-49.

212. *See supra* Sections I.A.3, I.B, I.D.

213. Michael P. Fischerkeller & Richard J. Harknett, *Deterrence is Not a Credible Strategy for Cyberspace*, 62 ORBIS 381, 390 (2017).

214. James Rundle, *Letting Businesses "Hack Back" Against Hackers Is a Terrible Idea, Cyber Veterans Say*, WALL ST. J. (July 8, 2021), https://www.wsj.com/articles/letting-businesses-hack-back-against-hackers-is-a-terrible-idea-cyber-veterans-say-11625736602 [perma.cc/Q26V-27S4]; Nicolas Winstead, *Hack-Back: Toward a Legal Framework for Cyber Self-Defense*, AMERICAN UNIV. ONLINE (June 26, 2020), https://www.american.edu/sis/centers/security-technology/hack-

convolute government investigation because hacking back may corrupt evidence.[215] Or, attacked entitles may find themselves confronting other nations directly without government support.[216] Furthermore, given the complexity of attributing cyberattacks, only resource-rich entities may vindicate cyberattacks, as smaller companies and the justice system cannot investigate and adjudicate all cyberattacks.[217] Given these enforcement challenges, cybercrime enforcement researchers found that less than one percent of cybercrimes lead to an arrest, meaning cybercriminals can act with near impunity.[218]

III. EXPANDING CISA'S RULEMAKING AND ENFORCEMENT AUTHORITY FOR NATIONAL DEFENSIVE CYBERSECURITY

Expanding CISA's authority to cybersecurity rulemaking and enforcement rectifies the three weaknesses identified above across the entire United States. Even though Congress created CISA to serve as the nation's cyber risk advisor,[219] CISA's current configuration limits the Agency's efficacy because the Agency cannot generally mandate reporting or cybersecurity measures such as multi-factor authentication or encryption.[220] Instead, CISA relies on other federal agencies like the FTC and SEC to collect cyber threat information.[221] Expanding CISA's rulemaking authority would rectify the lack of centralization by allowing CISA direct cyber infrastructure regulation, like the TSA can directly regulate critical pipelines.[222] Furthermore, equipping CISA with rulemaking and enforcement power affords CISA authority over private sector entities. And, rulemaking and enforcement authority limits reliance on self-regulation and cooperation while allowing for input from and collaboration with the private sector, non-profit organizations, and individuals through rulemaking notice and comment procedures. Enhancing CISA's rulemaking authority would also improve ex ante, defensive cybersecurity, rather than focusing on attributing or mitigating harm from cyberattacks that already occurred[223] because CISA could monitor and rectify systemic cyber vulnerabilities across sectors.

---

back-toward-a-legal-framework-for-cyber-self-defense.cfm [perma.cc/296C-Q3CB].

215. Porch, *supra* note 110, at 485.

216. *See id.*

217. *See* E.F.G. Ajayi, *Challenges to Enforcement of Cyber-Crimes Laws and Policy*, 6 J. INTERNET & INFO. SYS. 1, 4-11 (2016) (explaining that identifying cybercriminals and anonymity, jurisdictional complexity, extradition processes, nature of evidence, and investigation costs, among other issues, hinder judiciaries' cybercrime enforcement).

218. *See id. See generally* Allison Peters & Amy Jordan, *Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime*, 10 J. NAT'L SEC. L. POL'Y 487, 490-98 (2020).

219. *See supra* notes 104-05 and accompanying text.

220. *See supra* note 109 and accompanying text.

221. *See Cybersecurity Directives*, *supra* note 107 and accompanying text.

222. *See id.*

223. *See supra* Part II.

The United States needs "whole-of-the-nation" cybersecurity regulation to combat growing cyber threats with ex ante cyber defense,[224] but, given cyber infrastructures' complexity and interconnections, the nation's current sectoral cybersecurity approach obscures cyber vulnerabilities.[225] A genuine "whole-of-the-nation" cybersecurity regulator also considers the public good component of cyber defense because cyberattacks affect individuals and non-profit organizations as well as private sectors and critical infrastructures.[226]

Section III.A discusses the range of regulatory options and proposes that CISA needs rulemaking and enforcement authority for optimal national cybersecurity. In light of across sector cyber threats, Section III.B recommends centralizing cybersecurity authority with CISA. Section III.C argues that optimal cybersecurity requires considering cybersecurity's public good components outside of the private sector framework. Section III.D argues cyber defense, not ex post attribution or ransom sanctions, should guide federal cybersecurity regulations.

A. Range of Regulatory Tools

Congress authorizes federal agencies a range of different powers. As discussed in Section I.A, agencies like the FTC, SEC, and TSA issue binding regulations for specific private sectors, while the NIST cannot.[227] CISA's current configuration does not include rulemaking or enforcement power, limiting the Agency's ability to thwart cyberattacks.[228] Section III.A.1 argues rulemaking gives regulated entities ample notice of new regulations and allows all parties an opportunity to participate in regulation creation. Section III.A.2 argues giving CISA enforcement capabilities ensures regulated entities comply with rules and allows for more effective harm rectification than private litigation.

1. Rulemaking Functions.—Although rulemaking takes more time, information, and resources than one-off enforcement actions, rulemaking provides underutilized, indispensable benefits for defensive cybersecurity.[229] Rulemaking offers all people, from cybersecurity laypeople to experts, a mechanism for providing their knowledge and perspective to regulators to enhance regulation.[230] Agency rulemaking also gives regulated entities explicit notice of new rules, avoiding enforcement problems such as those the FTC encounters when its orders rely on vague or non-binding guidance materials.[231] Rulemaking enhances federal cybersecurity's quality, transparency, and legitimacy by following clear procedures, allowing input from regulated entities,

---

224. *See supra* Parts I, II.

225. *See id*.

226. *See supra* notes 15, 188 and accompanying text.

227. *See supra* Section I.A.

228. *See supra* notes 109-10 and accompanying text.

229. *See id*.

230. *See id*.

231. *See supra* notes 65-73 and accompanying text.

and providing explicit notice, unlike secretive national security programs.[232]

2. Enforcement Structures.—Federal Agencies also have different enforcement methods.[233] The DOJ has general enforcement responsibility for federal laws and houses the FBI, which gives the DOJ investigative power for its enforcement.[234] Other agencies, like the FTC, SEC, and TSA, have weaker enforcement authority that requires the DOJ's or other law enforcement agencies' cooperation before enforcing criminal regulations.[235] These intra-agency enforcement structures enhance efficiency by sharing expertise and resources and providing flexibility for complex inter-jurisdiction cases. Including multiple agencies also creates an inter-government oversight mechanism against enforcement and surveillance abuse, like the PRISM program.[236] Expanding CISA's enforcement authority beyond federal agencies through cooperation with other agencies, particularly the DOJ, would allow CISA more efficient response procedures against cyber risks and attacks.

B. Centralizing General Federal Cybersecurity Authority

Centralizing cybersecurity authority by expanding CISA's rulemaking and enforcement authority should not entail repealing any existing sectoral cybersecurity regulation. The FTC, SEC, NIST, Treasury, and DOJ's cybersecurity regulation and enforcement power serve specific functions like controlling unfair and deceptive trade practices,[237] monitoring public companies,[238] providing information,[239] overseeing currency in the United States,[240] and enforcing federal law.[241] Rather than demolish and re-create national cybersecurity, Congress should build upon the nation's existing security framework and expertise. This reform approach fosters continuity for currently regulated entities while addressing weaknesses in current federal cybersecurity.

As discussed in Section II.A, the lack of centralized general cybersecurity regulation confounds the nation's cyber defense.[242] Although Congress created CISA as the country's cyber threat monitor,[243] Congress did not give CISA adequate authority to assess systematic cyber threats given the sectoral approach

---

232. *See* AMBROGIO & STASZEWSKI, *supra* note 209 and accompanying text.
233. *See supra* Sections I.A-B.
234. *See supra* notes 111-13 and accompanying text.
235. *See supra* Section I.A.
236. *See supra* notes 33-36 and accompanying text.
237. *See supra* Section I.A.2.
238. *See supra* Section I.A.1.
239. *See supra* Section I.A.4.
240. *See supra* Section I.A.3.
241. *See supra* Section I.B.
242. *See supra* Section II.A.
243. *See supra* note 105 and accompanying text.

that CISA relies on through information sharing within the federal government.[244] Post-9/11 national security legislation centralized information, threat sharing, and response through the DHS that co-exists with other national security agencies like the DOJ and FBI.[245] CISA needs general rulemaking and enforcement power to assess risks across all cyber infrastructures regardless of sector, and proactively respond to cyber threats rather than rely on ex post harm mitigation.

A robust, general cybersecurity agency would also begin rectifying the separation between data privacy and cybersecurity. Since data breaches often result from cyberattacks,[246] CISA's enhanced ability to detect and prevent cyberattacks would also decrease data breaches and thus protect government and company secrets and individuals' privacy. Potential data breach victims would benefit from enhanced cybersecurity because ex ante cybersecurity would mitigate cyberattacks, which frequently result in data breaches that expose individuals' private information. Similarly, enhancing data privacy furthers cybersecurity because protecting personal and other private information makes hacking that information more difficult, reducing the likelihood of a successful cyberattack.

C. Focusing on Public Good, Not Businesses

Cyberattacks affect the entire nation, not just critical infrastructures and businesses.[247] Given cyber infrastructures' interconnections, maximizing cyber defense necessarily includes the whole nation because attacks on non-critical infrastructures or individuals can cascade into larger, more "critical" attacks.[248] Optimal ex ante cybersecurity must incorporate everyone, from individuals to critical infrastructures, because cyberattacks occur across all types of people, entities, and sectors. Creating genuinely "whole-of-the-nation" cybersecurity regulation requires considering the public good externalities from defensive cybersecurity. Giving CISA general rulemaking and enforcement power would allow the Agency to oversee cyber threats across individuals, organizations, and the private directly, rather than relying on sector-specific agencies or private sector cooperation information. Rulemaking would also enhance notice and transparency for regulated entities.[249]

Specifically, granting CISA rulemaking authority would allow the Agency to gather expertise, information, and perspectives from all interested parties, including individuals, through notice and comment procedures. Not only would notice and comment procedures ensure CISA receives as much information as possible to inform rulemaking, but rulemaking procedures would also give

---

244. *See supra* notes 108-10 and accompanying text.

245. *See supra* notes 167-80 and accompanying text.

246. *See* Garon, *supra* note 171 and accompanying text.

247. *See supra* notes 15, 188 and accompanying text.

248. *See supra* note 207 and accompanying text.

249. *See* AMBROGIO & GLEN STASZEWSKI, *supra* note 209 and accompanying text.

regulated entities ample notice of new regulations.[250] Therefore, CISA could avoid notice-based enforcement problems that impede the FTC's enforcement through rulemaking.[251] Centralizing rulemaking authority would increase cybersecurity regulation transparency because current patchwork regulations contradict each other.[252] Given the increase in domestic government surveillance in the United States post-9/11, cybersecurity transparency would foster CISA's rulemaking and enforcement legitimacy.[253]

D. Fostering Cyber Defense Across the Nation

Focusing on cyber defense through general cybersecurity regulation avoids attribution problems by preventing cyberattacks. Rather than waste resources contemplating retaliation and extradition against great powers like Russia and China for sponsoring cyberattacks,[254] ex ante cyber defense proactively prevents conflict by mitigating harm and thus the need for retaliation. The nation needs defensive, ex ante, and general cybersecurity to avoid attribution problems by mitigating cyber threats and damage. Current sector-specific regulators like the FTC and SEC cannot provide comprehensive cybersecurity because they are limited to private sector companies.[255] The Treasury's sanctions and proposed ACDC remain entity-specific and apply after an attack has already occurred.[256] Fostering general cyber defense through rulemaking benefits the entire nation by preventing cyberattacks prophylactically. In addition to maximizing cyber defense, avoiding attribution problems makes cyber regulation more accessible because individuals and smaller companies and organizations do not have the resources to hack back or receive a federal response. Expanding CISA's rulemaking authority would give the nation ex ante protection against cyberattack harm by sharing information and resources and enforcing entities' compliance with federal cybersecurity procedures and reporting rules.

CONCLUSION

Increasing cyberattacks show that the United States' patchwork federal cybersecurity regulation does not provide robust cyber defense across the entire nation.[257] Congress created CISA as the nation's cyber risk advisor,[258] but the Agency lacks the rulemaking and enforcement powers necessary to assess cyber

250. *See id*.
251. *See id*.; *supra* notes 65-73 and accompanying text.
252. *See supra* note 3 and accompanying text; *supra* Section II.A.
253. *See* AMBROGIO & STASZEWSKI, *supra* note 209 and accompanying text.
254. *See supra* notes 114-18 and accompanying text; *supra* Section II.C.
255. *See supra* Sections I.A.1-2.
256. *See supra* Sections I.A.3, I.D.
257. *See supra* notes 16-23 and accompanying text.
258. *See supra* notes 104-05 and accompanying text.

risks across the nation or maximize cybersecurity.[259] Granting CISA rulemaking and enforcement authority across sectors would greatly improve the whole nation's cybersecurity defense by mitigating current federal cybersecurity weaknesses.[260]

259. *See supra* notes 108-10, 161 and accompanying text; *supra* Part II.

260. *See supra* Part III.